Editor’s Note

IJRACSE : International Journal of Research in Advanced Computer Science Engineering is an international peer reviewed, open access, online journal published by Yuva Engineers for professionals and researchers in various disciplines of Engineering and Technology.IJRACSE is an is a science and Technology enrichment initiative designed for professionals & Researchers across the world. IJRACSE’s goal is to inspire young engineers and professionals to develop an interest in research and development, in doing so, recognise the importance and excitement of engineering, technology & management for the upliftment of entire Mankind.

IJRACSE solicits innovative research papers on the Engineering and Technological issues of the modern day world. The initiative brings together academic, industry, and students to a single-path, highly selective forum on the design, implementation, and applications of engineering.IJRACSE takes a broad view of Engineering to include any ideas that collectively addresses a challenge. We invite submissions covering a broad range of Engineering streams including conventional Computer Science Engineering, Programming, Algorithms, Circuits, Networking, Control Systems, Information Technology, Artificial Intelligence, Microprocessor, Microcontrollers, Computer Graphics & Multimedia.

You can be an Electronics engineering Professional/Researcher but you have an idea in computer science engineering, you are most welcomed to submit your idea. We are not restricting authors on the stream they belong to. Any one can submit paper on any topic he/she wish to. Authors can submit more than one paper, but has to submit separately. Multiple Authors can submit one paper as well.Policy Of the Journal: Submitted papers should be original and must have not been published nor submitted for review/publication to any other editorial. Please do not copy from Internet and submit them. We don’t encourage any kind of plagiarism. Try to put articles in your own words. Give credits and references to original authors and researchers where ever necessary.

Aim of the Journal:

The Journal Aims is to promote research and development of Engineering, Science, Technology and Management. The journal is working with the aim to provide a platform and publish original research work, review work, ideas and Designs.

Scope of the Journal:

We seek technical papers describing ideas, groundbreaking results and/or quantified system experiences. We especially encourage submissions that highlight real-world problems and solutions for it. Topics of interest include, but are not limited to, the following: Computer Science Engineering,

Parallel Processing and Distributed Computing, Foundations of High-performance Computing, Graph Theory and Analysis of Algorithms, Artificial Intelligences and Pattern/Image Recognitions, Neural Networks and Biomedical Simulations, Virtual Visions and Virtual Simulations, Data Mining, Web Image Mining and Applications, Data Base Management & Information Retrievals Adaptive Systems, Bifurcation, Biocybernetics & Bioinformatics, Blind Systems, Neural Networks &Control Systems, Cryptosystems &Data Compression, Evolutional Computation &Fuzzy Systems, Image Processing and Image Recognition, Modeling & Optimization, Speech Processing, Speech Synthesis & Speech Recognition, Video Signal Processing, Watermarking & Wavelet Transform, Computer networks & security, GIS, remote sensing & surveying and All topics related Computer Science.

The Features and Benefits of IJRACSE:

1. Fast and Easy procedure for publication of papers.
2. We follow Proper Peer review process and Editorial and Professional Ethics.
3. Each article/Paper will be published In the PDF version of Online Journal of IJRACSE. This paper may also be published in other associated Journals.
4. Permanent and Direct Link of your paper IJRACSE, So that you can share the link on your Linked, Facebook, Twitter etc pages to showoff to the world.
5. IJRACSE Provides Individual “Hardcopy of Certificate of Publication” to each author of the published paper.
6. IJRACSE is indexed in all major Indexing sites and databases.
7. Open access and free for anyone to view and download without registering.
8. The Most popular and widely read “Yuva Engineers” Monthly Print Magazine is our parent Publication. The Yuva Engineers Print Version is having a dedicated reader base of over 1 Lakh Readers. Selected Papers of the IJRACSE will be published in the print version aswell.

K.V.A.Sridhar
Editor & Publisher

INTERNATIONAL JOURNAL OF RESEARCH IN
ADVANCED COMPUTER SCIENCE ENGINEERING

Address : 11-4-650 Sovereign Shelters,
Redhills,Lakdikapul,
Hyderabad-500004.

Telephone : 040-66714050
Mobile +91 9866110776
Email Yuvaengineers@gmail.com
www.ijracse.com

Periodicity : Monthly

Language : English

Publisher,Editor & Owner K.V.A.Sridhar

Printed at Ratnaraj Printers
11-5-431/1, Redhills, Lakdikapul,
Hyderabad - 500004.

© All rights reserved. Nopart of the Publication may be reproduced by any mean without written permission from the publisher.

EDITORIAL & REVIEW BOARD

K.V.A.Sridhar, MSc(UK),BE,
Editor & Publisher.

Dr.R.Satya Raju, Ph.D,
Principal, Colleges of Arts and Commerce,
Andhra University.

Dr.Seema Shah, Ph.D, Principal & HOD,
Vidyalankar Institute Of Technology.

Dr.V.P.Chandramohan, BE, MBA, ME, Ph.D(IITD),
Assistant Professor, Mechanical Engg.Dept,
National Institute Of Technology Warangal.

Dr.Katta.Ravindra, MBA, M.Phil, Ph.D,
Prof Of Mrktg Mgmt School Of Mgmt and Acctg,
Hawassa University, Ethiopia.

N.Dinesh Kumar, AMIETEM.Tech, (Ph.D), LMISOI,
MIEEE,MIACSIT Associate Professor & HOD - EIE,
Vignan Institute Of Technology, Hyderabad.

Dr.B.Raveendranadh Singh, Ph.D,
Professor Of CSE & Principal
Visvesvaraya College Of Engineering & Technology.

Dr.A.Nagendra, Ph.D, M.Tech, HOD,
Dept Of Mechanical Engineering
St.Peter's Engineering College.

Dr.K.V.S.S.S.S.Sairam, BE, M.Tech, Ph.D
Principal, Scient Institute Of Technology.

Dr.Mir IqbalFaheem, Ph.D,M.Tech,HOD,Civil Engg,
Deccan College Of Engineering & Techology, Hyd.

K.Parvath Reddy, M.A, M.Phil, M.ED,Chairman
Dhruva Institute Of Engineering and Technology.

Dr.G.Vijay, M.T.M, M.Phil, Ph.d,
Dept of Business Management,
Chaitanya P.G College, Warangal.

Dr.SureshAkella, M.Tech, Ph.D,
Principal & Director R & D,
Shreyas Institute Of Engineering & Technology.

Dr.P.Mallesham, BE,ME,Ph.D, Principal,
Sri indu College Of Engineering and Technology.

Dr.M.Sarada Devi, M.B.A, Ph.D,
Department Of Commerce & Managment Studies,
Andhra University.

Kiran Kumar Jain, BE,M.Tech,(Ph.D), HOD EEE,
Bhaskar Engineering College.

Dr.K.Sathish, M.Tech, Ph.D,
Director, Sri Chaitanya Technical Campus College Of
Engineering & Technology.

Dr.S.Krishna Mohan Rao, Ph.D , Principal,
Siddhartha Institute Of Engineering & Technology.

Ramesh Bandaru, M.Tech,
Asst.Prof, Dept.Of CSE, Aditya Institute Of
Technology and Management, (AITAM), Tekkali.

Dr.Surender Adki, Ph.D,
Principal & Reader in Public Administration,
Vivekvardhini.(AN) College Of Arts & Commerce.

Dr.Bhaskar Rao.Netha, LLB, MBA,Ph.D(OSM),
Principal, Sri Indu Institute Of Management.

Pradeep Kumar V, Business Head, India Business
Unit, Charter Gobal, India.

Suresh Aadepu,
Associate Professor,Dept of Mechanical Engineering,
K.G Reddy College of Engineering and Technology.

Prof.M.Ramakanth Reddy,Principal, Vishwa Bharathi
Institute Of Technology and Sciences.

Dr.J.V.Ravindra, Ph.D, MIEEE, MIETE, MIE,
Principal, Vardhaman College Of Engineering.

Dr.M.Sreedhar Reddy, MTECH, Ph.D, Principal,
Samskruti College Of Engineering & Technology.

S.Dharma Siva,
C.E.O & Co-Founder Techno Talent Group,India.

Dr.J.Varaprasad Reddy,
Director,MBA,NET,Ph.D,
TKR Institute Of Management & Sciences.

Khaja Mohinuddin,MSC,M.Phil,
Principal, Green Fort Engineering College.

P. Parthsaradhy, Associate Director,
Guru Nanak Institutions Technical Campus.

Dr.P.Ram Mohan Rao,
Principal,Teegala Krishna Reddy Engineering College.

A.K.V.V.M. Sastry,
Assistant Professor in M.B.A,
Vivek Vardhini School of Business Management.

Dr. B. Srinivasa Rao, M.Tech.,Ph.D, MIAENG,
Sankethika Vidya Parishad Engineering College.

Dr. Prasanna Khadkikar,
Sr Faculty And HoD Commerce
Vivek Vardhini (A.N) College.

Dr. A. Srinivasa Rao,M.Tech.,Ph.D,
Aditya Institute Of Technology and Management.

Dr Sohel Ahmed, MBA, Ph.D, M.A., M.Phil., (Ph.D.)
Associate Professor, Dept. Of Humanities & Sciences,
Green Fort Engineering College.

Dr. D. Vijay Kumar, B. E (Civil), M.E (public health),
M.E (Transportation Engg), Ph. D, M.B.A (Ph.D)
Principal, Sri Sivani Institute of Technology.

Rama Krishna Chandaka, MBA, (Ph.D), Chief Advisor.

Graphic Designer : Mohammed Younus, Bsc(Msc.s).

Inside

Call For Papers: IJRACSE solicits innovative research papers on Engineering Technological, and Management issues of CSE. The initiative brings together academic, industry, and students to a single-path, highly selective forum on the design, implementation, and applications of engineering & management.

Ten Step Process for Submission:

Step 1..Covering Letter to be Attached as Below:

Dear Sir/Madam,
Please find my submission of Technical paper entitled '____________________' with reference to your Call for Papers.
I hereby affirm that the contents of this Technical Paper are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it under review for publication elsewhere.
I affirm that all the authors have seen and agreed to the submitted version of the Technical Paper and their inclusion of names as co-authors.
Also, if my/our Technical paper is accepted, I/We agree to comply with the terms and conditions as given on the website of the journal & you are free to publish our contribution in any of your journals/Magazines and website.
Name of the Author: Signature: Designation: College/Organisation: Full address & Pin Code:
Mobile Number (s):   Landline Number (s):   E-mail Address: Alternate E-mail Address:

Step 2... The Technical Paper should be submitted in Hard copy and aswell as Soft copy. Soft copy should be in CD/DVD. Your soft copy will be published on website giving credits to you.

Step 3... AUTHOR NAME (S) & AFFILIATIONS: The author (s) full name, designation, affiliation (s),College/Institution, Year & Department, Guide Name and Designation(If Any), address, mobile / landline numbers, and email / alternate email address should be in italic & 12-point in Georgia Font. It must centered underneath the title.

Step 4..ACKNOWLEDGMENTS: Acknowledgments can be given to reviewers, funding institutions, etc., if any.

Step 5..ABSTRACT: Abstract should be in fully italicized text, not exceeding 250 words. The abstract must be informative and explain the background, aims, methods, results & conclusion in a single para. Abbreviations must be mentioned in full.

Step 6... FORMAT: Manuscript must be in BRITISH ENGLISH prepared on a standard A4 size PORTRAIT SETTING PAPER. It must be prepared on a single space and single column with 1⍰ margin set for top, bottom, left and right. It should be typed in 12 point Georgia Font with page numbers at the bottom and centre of every page.
All Headings and Sub-Headings must be bold-faced, aligned left and fully capitalized and typed in 12 Point Gerogia Font.
Figures and Table: Please do not copy figures and tables from net. Draw them on your own. Sources of data should be mentioned below the table/figure. It should be ensured that the tables/figures are referred to from the main text.

Step 7...REFERENCES: The list of all references should be alphabetically arranged. The author (s) should mention only the actually utilised references in the preparation of manuscript and they are supposed to follow Harvard Style of Referencing.

Step 8...HOSTING & CERTIFICATION FEE: Send your hard copy+Soft copy along with 1500 rupees DD favoring "Yuva Engineers" Payable at "Hyderabad"

Step 9....ADDRESS TO BE POSTED: Send your entries to "Yuva Engineers, D.NO: 11-4-650, 204 Sovereign Sheleters, Redhills, Lakdikapul, Hyderabad – 500004

Step 10... Details Sheet: Please Attach a separate sheet with your details: Name, Address, email, Telephone number, Branch of Engineering, Semester studying, College name and Address. (If more than one student is submitting the paper, Attach separate sheet with details)

Volume No:1, Issue No:1 (June-2015)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

Methods on How to Maintain Safety While We Are Exchanging the Data on Web Services, So that the Unauthorized Entities Should Not Be Able To Access the Information within the Message

Sudheer Reddy.G

Assistant Professor, Department of Computer Science & Engineering,
Spoorthy Engineering College, Hyderabad.

Abstract:

Web Services are a loosely-coupled, language-neutral, platform- independent way of linking applications within organizations, across enterprises, and across the Internet. With web services we can exchange data between different applications and different platforms. While we are exchanging the data, the unauthorized entities should not be able to access the information within the message. In this paper, we discuss the areas of safety and how to maintain that safety. It also describes the benefits of the web services and the standards which are used on the web services.

Keywords:

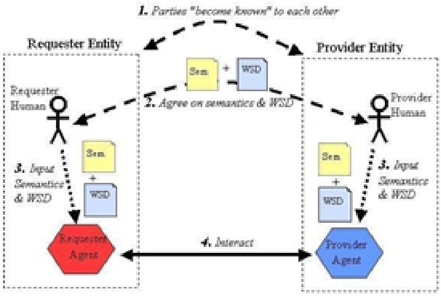
Web service components, Benefits of Web service, and Web Services Safety.

I.Introduction:

A Web service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (WSDL).Other systems interact with the web service in a manner prescribed by its description using SOAP message, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards.A Web service is an abstraction notion that must be implemented by a concrete agent. The agent is the concrete piece of software or hardware that sends and receives messages.

• Overview of Engaging a Web Service

There are many ways that a requester entity might engage and use a web service. In general, the following steps are required, as illustrated in figure-1.



1.The requester and provider entities Become known to each other or at least one becomes known to the other.

2.The requester and provider entities somehow agree on the service description and semantics that will govern the interaction between the requester and provider agents.

3.The service description and semantics are realized by the requester and provider agents

4.The requester and provider agents exchange the messages, thus performing some task on behalf of the requester and provider entities.

II. COMPONENTS OF WEB SERVICES:

The basic Web services platform is XML + HTTP . All the standard Web services works using the following components:

• SOAP (Simple Object Access Protocol)

SOAP is an XML-based protocol for exchanging information between computers. It is a communication protocol between applications, standard format for sending messages to communicate via Internet. It is platform independent, Language independent, simple and extensible.

• UDDI (Universal Description, Discovery and Integration)

UDDI is a specification for a distributed registry of Web services, platform independent and open framework. It can communicate via SOAP, CORBA, Java RMI protocol. It is an open industry initiative enabling business to discover each other and define how they interact over the Internet.

• WSDL (Web Services Description Language).
It is an XML based protocol for information exchange in decentralized and distributed environments.

III.Benefits of Web Services:

• Exposing the function on to network

Web services allows us to expose the functionality of our existing code over the network. Once it is exposed on the network, other application can use the functionality of our program.

• Connecting Different Application

Web services allows different applications using different languages to talk to each other and share data and services among them selves. So, Web services is used to make the application platform and technology independent.

• Standardized Protocol

Web services uses standardized industry protocol for the communication.

• Loosely Coupled Applications

Web services are self-describing software modules which encapsulates discrete functionality. Web services can be developed in any technologies(like C++, Java, .NET, PHP, Perl etc.) and any application or Web services can access thes services. So, the Web services areloosely coupled application and can be used by application developed in and technologies.

• Web Services are Self Describing

Web services are self describing applications, which reduces the software development time.

• Automatic Discovery

Web services automatic discovery mechanism helps the business to easy find the Service Providers. This also helps our customer to find our services easily.

• Business Opportunity

Web services has opened the door to new business opportunities by making it easy to connect with partners.

IV. WEB SERVICES SAFETY:

In securing Web Services, there are five fundamental areas to consider: Message Level Protection, Message Privacy,Parameter Checking, Authentication and Authorization.

• Message Privacy :

The Message privacy deals with the confidentiality of a message. The Confidentiality is concerned with protecting the privacy of the message contents. A message is considered to have remained confidential if no service or agent in this message path not authorized to do so viewed its contents. The message header contains the information of XML Signature and Token , shown in the figure-2

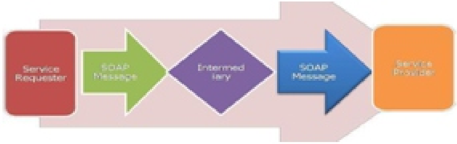


Fig-2: SOAP message in Transit

To ensure confidentiality an encryption scheme must be implemented. Once the message has been received by anentity (intermediary) it is decrypted in its entirety.The XML Encryption standard provides the necessary framework for accomplishing this task. The XML Encryption allows for the encryption of any combination of the message body, header, attachments and sub-structures.When a message or part of a message is encrypted, the encryption information can be made available in the message header. This information is useful for complex services since each Web Service in the claim will need to know how to decrypt the section of the message relevant to their services. This information should not be the actual key to decrypt the message.

For example, when a requester encrypts a message body and XML signature information in the header, it may then specify in the header that it has used the providing service's public key. A public key allows for the encryption of data but only the private key may decrypt the data. Once the provider receives the message it sees that the message has been encrypted using its public key. The provider then decrypts the message using its private key.XML Encryption allows multiple different keys to be used with in a message to encrypt different sections, elements of the message.

• Message Level Protection

Message Level Protection has to do with message integrity. Integrity means ensuring that a message's contents have not changed during transmission. This means being able to detect when a SOAP message (message) has been modified from its original state and the ability to guarantee that the contents have not been modified. This is done by creating a message digest.To ensure message integrity, a technology is required that is capable of verifying that the message received by a service is authentic in that it has not been altered in any manner since it first was sent. XML-Signature provides piece of information that represents a digital signature. This signature is tied to the content of the document so that verification of the signature by the receiving service only will succeed if the content has remained unaltered since it first was sent.The figure-3 illustrate the XML-Encryption canbeapplied to parts of a soap header, as well as the contents of the SOAP body. When singing a document , the XML-signature can reside in the SOAP-header.

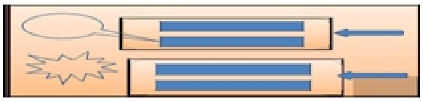


Fig-3: A digitally signed SOAP message containing encrypted data.

There are several Token options for signing a message. These options fall under one of two categories; they can either be endorsed or unendorsed.
(1)Endorsed: An endorsed token is one which the claims of the token can be validated by a trusted authority. An example ofthis kind of Token is a X.509 certificate.
(2)Unendorsed: An unendorsed Token is one which the claims may not be validated by a trusted authority. An example of thiskind of token is a username-password Token.

Message Validity:

Message Validity is ensuring that the contents of a message are appropriate to the service and that they are well formed. Checking the contents of a message can be subdivided into two categories; Verifying data types and checking for malicious code. Verifying that the data types passed to an operation are those which the services are expecting is straight. Checking for malicious code within the message is not so straight forward.Malicious code within a message ca appear as part of the XML message or as parameters to be passed to operations. XML viruses and XML worms are commonly passed within the contents of any XML document or message. Even after verifying that the parameters within a message are appropriate for the operation(s), their may be malicious code present.Ensuring that a message is well-formed is another step in Message Validity. Since the messages are in XML, it is possible that a message contains a circular-reference. A circular-reference may appear maliciously or through poor programming. Circular-references cause a system to encounter a run-out-of-memory error and shutdown. When done maliciously this is known as a denial-of-service attack. Proper parsing of a message will catch nested loops.

• Authentication

Authentication requires that a message being delivered to a recipient prove that the message in fact from the sender that it claims to be. In other words, the service must provide proof that its claimed identity is true.In its simplest form, authentication could be a username and password combination. However, this is only possible if there is already a relationship between the requester and provider. Because of the distributed nature of web services, a requester may be previously unknown to the provider.When an unknown requester authenticates it sends information about themselves to the provider. This information is known as credentials. For the unknown requester, the authentication can be achieved through a trusted authority, who issue certificates which can be used for authentication. A provider can evaluate the certificate and contact the trusted authority for verification.However, there may be an intermediate service contacting the provider on behalf of the requester and once established the requester and provider will communicate.

• Authorization

In organizations, highly sensitive data and information must be protected with access control systems. These control systems allow defining and controlling which users are authorized to access specific applications and data but prohibit the access of unauthorized users.Authentication is the granting of rights, which includes the granting of access based on access rights. Once authenticated, the recipient of a message may need to determine what the requestor is allowed to do.

An access control implementation compares access control information such as the rights of the requestor with the policies or permission needed to access the resource. 0If the rights of the requester dominate the control policy; then access can be granted; otherwise access is denied.The two most common access control implementations are ACL(Access Control List) used in the Unix environment for file and directory safety and RBAC (Role Based Access Control) which consists of objects, operations, permissions, roles, users and system and Administrative functions(System functionality, administrative operations and reviews).

V.Conclusion:

Using web services we can exchange data between different applications and different platforms. While exchanging the data, the unauthorized person can access the information within the message. Hence, to secure the Web Services, we have to consider five fundamental areas: Message Level Protection, Message Privacy, Parameter Checking, Authentication and Authorization. This paper has presented an overview of how to secure the Web Services in all those areas. In Future, we will develop a safety tool for Web Services

References:

1.YUE Kun+, WANG Xiao-Ling, “Underlying Techniques for Web services : a survey”, Department of computer science and Engineering, Fudan University, Shanghai, China.

2.Thomas Erl, “ Service-Oriented Architecture – Concepts, Technology and Design”, PearsonEducation,Inc.

3.Richard S.Patterson, John A.Miller, University of Georgia, “ Safety and Authorization Issues in HL 7 Electronic Health Records: A Semantic Web Services Based Approach”,International Journal of Web Services research.

4.KarthikeyanBhargavan, CeedricFournet, Andrew D.Gordin, & Riccardo Pucella,”TulaFale : A safety Tool for Web Sevices”, Microsoft research.

5.WebServices, www.w3schools.com/webservices

6.Web services Safety – www.tutorialpoint.com/webservices

7.SOA and Web Service – www.roseindia.net/web services 8. Webservices – http://msdn.micosoft.com/en-us/library/ .

Volume No:1, Issue No:1 (June-2015)

International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

A new decision tree algorithm IQ Tree for class classification problem in Data Mining

C.V.P.R.Prasad
Research Scholar,
Acharya Nagarjuna University,
Guntur, Andhra Pradesh, India.

Dr. Bhanu Prakash Battula
Associate Professor,
Vignan College,
Andhra Pradesh, India.

ABSTRACT :

Data mining and knowledge discovery is used for discovery of hidden knowledge from large data sources. Decision trees are one of the most famous classification techniques with simple and efficient generalization technique. This paper presents a new decision tree algorithm IQ Tree for class classification problem. The IQ Tree assumes using an inter quartile range conversion of attributes with C4.5 as the base algorithm for performing induction can improve all the measures such as accuracy, tree size.

Keywords:

DataMining, Classification, Decision Tree,inter quartile range.

1. INTRODUCTION:

In Machine Learning community, and in data mining works, classification has its own importance. Classification is an important part and the research application field in the data mining [1].A decision tree gets its name because it is shaped like a tree and can be used to make decisions. ―Technically, a tree is a set of nodes and branches and each branch descends from a node to another node. The nodes represent the attributes considered in the decision process and the branches represent the different attribute values.

To reach a decision using the tree for a given case, we take the attribute values of the case and traverse the tree from the root node down to the leaf node that contains the decision.” [2]. A critical issue in artificial intelligence (AI) research is to overcome the so-called ―knowledge-acquisition bottleneck” in the construction of knowledge-based systems. Decision tree can be used to solve this problem. Decision trees can acquire knowledge from concrete examples rather than from experts [3]. In addition, for knowledge-based systems, decision trees have the advantage of being comprehensible by human experts and of being directly convertible into production rules [4].

2. LITERATURE REVIEW :

In Data mining, the problem of decision trees has also become an active area of research. In the literature survey of decision trees we may have many proposals on algorithmic, data-level and hybrid approaches. The recent advances in decision tree learning have been summarized as follows: A parallel decision tree learning algorithm expressed in MapReduce programming model that runs on Apache Hadoop platform is proposed by [5].A new adaptive network intrusion detection learning algorithm using naive Bayesian classifier is proposed by [6]. A new hybrid classification model which isestablished based on a combination of clustering, feature selection, decision trees, and genetic algorithmtechniques is proposed by [7]. A novel roughest based multivariate decision trees (RSMDT) method in which, the positive region degree of condition attributes with respect to decision attributes in rough set theory is used for selecting attributes in multivariate tests is proposed by [8]. A novel splitting criteria which chooses the split with maximum similarity and the decision tree is calledmstreeis proposed by [9].

An improvedID3 algorithm and a novel class attribute selection method based on Maclaurin-Priority Value First method is proposed by [10]. A modified decision tree algorithm for mobile user classification, which introducedgenetic algorithm to optimize the results of the decision tree algorithm, is proposed by [11].

Volume No:1, Issue No:1 (June-2015)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

A new parallelized decision tree algorithm on a CUDA (compute unified device architecture), which is a GPGPU solution provided by NVIDIA is proposed by [12]. A Stochastic Gradient Boosted Decision Trees based method is proposed by [13].

A modified Fuzzy Decision Tree for the fuzzy rules extraction is proposed by [14].Obviously, there are many other algorithms which are not included in this literature. A profound comparison of the above algorithms and many others can be gathered from the references list.

3. THE PROPOSED APPROACH :

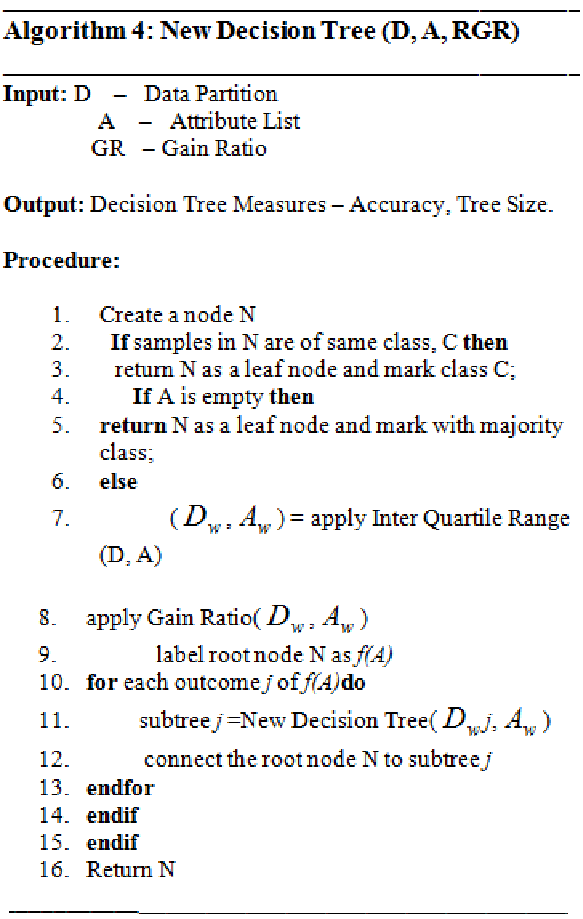
In this Section, we investigate to propose a new decision tree induction algorithm known as Inter Quartile (IQ) Range Decision Tree. Our IQ Decision Tree induction method depends on inter quartile ranges which was descried in the above section. We assume that the subset of the training data is small, i.e. it is computationally cheap to act on such a set in a reasonable time. We focus on a set of improved attribute range filters using attribute transformations.

Next, we try to adapt and deploy them as IQ Tree components. Since the IQ Tree scheme is based on a restricted list of candidates, this list could be represented by features that seems to be relevant or those that might provide incremental usefulness to the selected feature subset.

For the IQ Tree construction stage we opt for selection scheme capable of generating attribute ranking. Hence, the weights associated to features will serve as one of the selection criterion in the new heuristic function for inducing decision trees. The next stage of IQ Tree tries to consider both entropy and weights for splitting of attributes.

The quality of solution fine-tuning, mainly, depends on the nature of the filter involved and the parameters of attribute transformation. The following algorithm, detail different design alternatives for both attributes transform and filter procedure search for IQ Tree components.

The algorithm for IQ decision tree is shown below



Algorithm 4: New Decision Tree (D, A, RGR)

Input: D – Data Partition
A – Attribute List
GR – Gain Ratio

Output: Decision Tree Measures – Accuracy, Tree Size.

Procedure:

```
Create a node N
 If samples in N are of same class, C then
  return N as a leaf node and mark class C;
    If A is empty then
return N as a leaf node and mark with majority
class;
else
        ( $D_w$ , $A_w$ ) = apply Inter Quartile Range
(D, A)
apply Gain Ratio( $D_w$ , $A_w$ )
          label root node N as f(A)
for each outcome j of f(A) do
        subtree j =New Decision Tree( $D_w j$, $A_w$ )
         connect the root node N to subtree j
endfor
endif
endif
Return N
```

The algorithm: IQ Tree can be explained as follows:

The inputs to the algorithm are data partition “D”, attribute set “A” and splitting criteria gain ratio “GR”. The output of the algorithm will be the average measures such as accuracy and tree size produced by the IQ Tree method. The algorithm begins with the create node for same class. In the next stage, attribute rages are applied to the inter quartile for transformation. In the later on stage, the transformed dataset is applied for the splitting criteria gain ratio for decision tree induction. The induced decision tree is applied for the tree pruning process for generalization of the tree. In the final the measures for decision tree validation i.e accuracy ad tree size are generated.

4. RESULTS AND DISCUSSION:

We experimented with 10 standard datasets from the UCI repository, these datasets are standard benchmark imbalanced datasets used in the context of supervised learning. The goal is to examine whether the proposed IQ Tree achieve better predictive performance than a number of existing standard learning algorithms.

Volume No:1, Issue No:1 (June-2015)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

We compared the above method with the C4.5, BPN, REP, CART and NB Tree state-of-the-art metric learning algorithms. In all the experiments we estimate accuracy using 10-fold cross-validation and control for the statistical significance of observed differences using t-test (sig. level of 0.05). In Table 3 and 4, we present the results of the comparison between C4.5, BPN, REP, CART, NB Tree and IQ Tree.

From these results we can make several observations. The developed IQ Tree compared with C4.5, REP, CART, NB Tree generally given competitive results; the advantage of our methods is most visible in the balance, diabetes, glass, ionosphereand sonar datasets. Finally, the method that most often win is IQ Tree.

Table 3 Summary of tenfold cross validation performance for Accuracy on all the datasets

S.No	Datasets	C4.5	REP	CART	NB Tree	IQ Tree
1.	Balance-scale	77.82●	78.54●	78.73●	75.96●	97.24
2.	Breast-cancer	74.28●	69.35●	70.22●	70.99●	98.7
3.	Pima_diabetes	74.49●	74.46●	74.56●	74.96●	95.25
4.	Glass	67.63●	65.54●	71.26●	69.84●	76.48
5.	Heart-statlog	78.15●	76.15●	78.07●	80.93●	91.51
6.	Ionosphere	89.74●	89.46●	88.87●	90.03●	93.16
7.	Iris	94.73●	93.87●	94.20●	93.47●	95.19
8.	Sonar	73.61●	72.69●	70.72●	77.11●	82.82
9.	Vehicle	72.28●	70.18●	69.91●	70.98●	86.64
10.	Waveform	75.25●	76.57●	76.65●	79.84●	89.66
Win/Tie/Loss		**(10/0/0)**	**(10/0/0)**	**(10/0/0)**	**(10/0/0)**	

● Bold dot indicates the win of proposed method; ○ Empty dot indicates the loss of proposed method.

Table 4 Summary of tenfold cross validation performance for Tree Size on all the datasets

S.No	Datasets	C4.5	REP	CART	NB Tree	IQ Tree
1.	Balance-scale	82.20●	42.36○	55.28●	17.38○	30.64
2.	Breast-cancer-w	23.46●	13.76●	15.90●	5.68○	9.58
3.	Pima_diabetes	43.40○	30.98○	17.36○	5.18○	27.58
4.	Glass	46.16●	19.70○	21.16○	10.0○	39.98
5.	Heart-statlog	34.64●	14.78●	15.36●	9.62○	19.38
6.	Ionosphere	26.74●	8.76○	8.42○	16.20○	18.42
7.	Iris	8.28●	5.84○	7.40○	4.38○	10.90
8.	Sonar	27.90●	10.20○	10.50○	13.74○	26.46
9.	Vehicle	138.0●	58.52○	92.54○	57.70○	84.62
10.	Waveform	591.94●	167.24○	98.32○	94.48○	290.44
Win/Tie/Loss		**(9/0/1)**	**(2/0/8)**	**(3/0/7)**	**(0/0/10)**	

● Bold dot indicates the win of proposed method; ○ Empty dot indicates the loss of proposed method.

Table 3and4 presents the comparative results of proposed algorithm IQ Tree against C4.5, REP, CART and NB Tree. The value in the table; example: "11/0/2" specifies that the proposed algorithm has registered 11 wins, 0 ties and 2 losses against compared algorithm for that specified measure. One can observe from the table 3 and 4 that our proposed algorithms have registered good number of wins against the compared algorithms on all the datasets. These results suggest that in the majority of the high dimensional datasets, the feature interactions are not important, and hence the methods that do not account for feature interactions have in general better performances. Alternatively, it might suggest that stronger regularization is needed. Moreover, it is interesting to note that the cases for which the good performance are difficult classification problems from the UCI datasets. This hints that there might be a bias of method development towards methods that perform well on UCI datasets; however, one can argue that they are really representative of the real world.These results are remarkable since IQ Tree, which is based on a simple idea, performs equally well as the more elaborate standard learning algorithm that has been reported to consistently outperform other metric learning techniques over a number of non-trivial learning problems. Finally, we mention that the surprisingly poor performance of IQ Tree on sonar, vehicle and vowel datasets in tables 4, might be explained by the fact that its conversion function is not convex and hence it is sensitive to the unique properties of the datasets.

In overall, from all the tables and figures we can conclude that our proposed IQ Tree have given good results when compared to benchmark algorithms. The unique properties of datasets such as size of the dataset and the number of attributes will also effect on the results of our proposed IQ Tree. The above given results are enough to project the validity of our approach and more deep analysis should be done for further analysis.

5. CONCLUSION:

This paper presents a new decision tree algorithm IQ Tree for class classification problem. The IQ Tree assumes using an inter quartile range conversion of attributes with C4.5 as the base algorithm for performing induction can improve all the measures such as accuracy, tree size. The experiments conducted with IQ Tree specify that improved performance can be achieved. We have conducted experiments on 10 datasets from UCI which suggest that IQ Tree can quickly remove redundant, irrelevant and weak attributes as long as the properties of the dataset are normal.

Excellent improvement in measures on some natural domain datasets shows the compatibility of IQ Tree approach on real-time applications. One of the shortcomings seen in IQ Tree is when used for datasets with unique properties; Because IQ Tree will not consider unique properties of datasets for removing instances from data source. Finally, we can conclude that IQ Tree can be a good contribution as a decision tree induction method for efficient learning of the varied datasets.

References:

1.Juanli Hu, Jiabin Deng, Mingxiang Sui, A New Approach for Decision Tree Based on Principal Component Analysis, Proceedings of Conference on Computational Intelligence and Software Engineering, page no:1-4, 2009.

2.Shane Bergsma, Large-Scale Semi-Supervised Learning for Natural Language Processing, PhD Thesis, University of Alberta, 2010.

3.J. Durkin. Expert Systems: Design and Development, Prentice Hall, Englewood Clis, NJ, 1994.

4.J. Quinlan. C4.5 Programs for Machine Learning, San Mateo, CA:Morgan Kaufmann, 1993.

5.VasilePurdila, Ştefan-Gheorghe Pentiuc" MR-Tree - A Scalable MapReduce Algorithm for Building Decision Trees", Journal of Applied Computer Science & Mathematics, no. 16 (8) /2014, Suceava.

6.Dewan Md. Farid, NouriaHarbi, and Mohammad Zahidur Rahman" Combining naive bayes and decision tree for adaptive intrusion detect", International Journal of Network Security & Its Applications (IJNSA), Volume 2, Number 2, April 2010.

7.Mohammad Khanbabaei and Mahmood Alborzi" THE USE OF GENETIC ALGORITHM, CLUSTERING AND FEATURE SELECTION TECHNIQUES IN CONSTRUCTION OF DECISION TREE MODELS FOR CREDIT SCORING", International Journal of Managing Information Technology (IJMIT) Vol.5, No.4, November 2013. DOI : 10.5121/ijmit.2013.5402

8.Dianhong Wang, Xingwen Liu, Liangxiao Jiang, Xiaoting Zhang, Yongguang Zhao" Rough Set Approach to Multivariate Decision Trees Inducing?", JOURNAL OF COMPUTERS, VOL. 7, NO. 4, APRIL 2012.

9.Xinmeng Zhang, Shengyi Jiang "A Splitting Criteria Based on Similarity in Decision Tree Learning", JOURNAL OF SOFTWARE, VOL. 7, NO. 8, AUGUST 2012.

10.Ying Wang, Xinguang Peng, and Jing Bian" Computer Crime Forensics Based on Improved Decision Tree Algorithm", JOURNAL OF NETWORKS, VOL. 9, NO. 4, APRIL 2014.

11.Dong-sheng Liu, Shujiang Fan" A Modified Decision Tree Algorithm Based on Genetic Algorithm for Mobile User Classification Problem", Scientific World Journal, Volume 2014, Article ID 468324, 11 pages, http://dx.doi.org/10.1155/2014/468324, Hindawi Publishing Corporation.

12.Win-Tsung Lo, Yue-Shan Chang, Ruey-Kai Sheu, Chun-Chieh Chiu and Shyan-Ming Yuan," CUDT: A CUDA Based Decision Tree Algorithm", e Scientific World Journal, Volume 2014, Article ID 745640, 12 pages, http://dx.doi.org/10.1155/2014/745640. Hindawi Publishing Corporation.

13.Tarun Chopra, JayashriVajpai" Fault Diagnosis in Benchmark Process Control System Using Stochastic Gradient Boosted Decision Trees", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-1, Issue-3, July 2011.

14.S.V.S. Ganga Devi" FUZZY RULE EXTRACTION FOR FRUIT DATA CLASSIFICATION", COMPUSOFT, An international journal of advanced computer technology, 2 (12), December-2013 (Volume-II, Issue-XII).

15.HamiltonA. Asuncion D. Newman. (2007). UCI Repository of Machine Learning Database (School of Information and Computer Science), Irvine, CA: Univ. of California [Online]. Available: http://www.ics.uci.edu/mlearn/MLRepository.html

16.Witten, I.H. and Frank, E. (2005) Data Mining: Practical machine learning tools and techniques. 2nd edition Morgan Kaufmann, San Francisco.

17.J. Quinlan. Induction of decision trees, Machine Learning, vol. 1, pp. 81C106, 1986.

18.L. Breiman, J. Friedman, R. Olshen, and C. Stone, Classification and Regression Trees. Belmont, CA: Wadsworth, 1984.

19.Nitesh V. Chawla et. al. (2002). Synthetic Minority Over-sampling Technique. Journal of Artificial Intelligence Research. 16:321-357.

Volume No:1, Issue No:1 (June-2015)

International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Surveillance and Privacy Protection in MSNs and OSNs

M Santosh Reddy
B.Tech Student,
Department of CSE,
TKR College of Engineering & Technology.

M Saikrishna
B.Tech Student,
Department of CSE,
TKR College of Engineering & Technology.

K Surya Prakash Reddy
B.Tech Student,
Department of CSE,
TKR College of Engineering & Technology.

Dr. K.Venkatesh Sharma
Professor,
Department of CSE,
TKR College of Engineering & Technology.

Abstract:

Mobile social networking is social networking where individuals with similar interests converse and connect with one another through their mobile phone and/or tablet. Much like web-based social networking, mobile social networking occurs in virtual communities. A current trend for social networking websites, such as Facebook, is to create mobile apps to give their users instant and real-time access from their device.

Safety issues (including security, privacy, Surveillance and trust) in Online and mobile social networks are concerned about the condition of being protected against different types of failure, damage, error, accidents, harm or any other non-desirable event, while mobile carriers contact each other in mobile environments.

However, lack of a protective infrastructure in these networks has turned them in to convenient targets for various perils. This is the main impulse why OSNs and MSNs carry disparate and intricate safety concerns and embrace divergent safety challenging problems.

Surveillance is the monitoring of the behavior, activities, or other changing information, usually of people for the purpose of influencing, managing, directing, or protecting them.

Surveillance is also considered and discussed in this paper. The rationale behind this work paper is to investigate the threats to privacy that come up while users not have a good judgment of privacy consciousness and apprehension when using social networking sites. This particular approach, though, clashes with users' increasing privacy concerns regarding revealing their individual profiles to absolute unfamiliar persons.

Keywords:

Online Social Networks(OSNs), Mobile Social Networks(MSNs), Privacy, Surveillance, Individual Profiles, Privacy Protection, Information encryption.

Introduction:

Privacy is one of the friction points that emerge when communications get mediated in Online Social Networks (OSNs). Different communities of computer science researchers have framed the 'OSN privacy problem' as one of surveillance, institutional or social privacy. In tackling these problems they have also treated them as if they were independent. We argue that the different privacy problems are entangled and that research on privacy in OSNs would benefit from a more holistic approach.

In this article, we first provide an introduction to the surveillance and social privacy perspectives emphasizing the narratives that inform them, as well as their assumptions, goals and methods. We then juxtapose the differences between these two approaches in order to understand their complementarity, and to identify potential integration challenges as well as research questions that so far have been left unanswered. A social networking service is a platform to build social networks or social relations among people who share interests, activities, backgrounds or real-life connections.

A social network service consists of a representation of each user (often a profile), his or her social links, and a variety of additional services. Social networks are web-based services that allow individuals to create a public profile, to create a list of users with whom to share connections, and view and cross the connections within the system.

Most social network services are web-based and provide means for users to interact over the Internet, such as e-mail and instant messaging. Social network sites are varied and they incorporate new information and communication tools such as mobile connectivity, photo/video/sharing and blogging.More and more, the line between mobile and web is being blurred as mobile apps use existing social networks to create native communities and promote discovery, and web-based social networks take advantage of mobile features and accessibility. As mobile web evolved from proprietary mobile technologies and networks, to full mobile access to the Internet, the distinction changed to the following types:

1) Web based social networks being extended for mobile access through mobile browsers and smartphone apps, and

2) Native mobile social networks with dedicated focus on mobile use like mobile communication,location-based services, and augmented reality, requiring mobile devices and technology. However, mobile and web-based social networking systems often work symbiotically to spread content, increase accessibility and connect users from wherever they are.

Privacy concerns with social networking services have been raised growing concerns amongst users on the dangers of giving out too much personal information and the threat of sexual predators. Users of these services also need to be aware of data theft or viruses. However, large services, such as MySpace and Netlog, often work with law enforcement to try to prevent such incidents.

In addition, there is a perceived privacy threat in relation to placing too much personal information in the hands of large corporations or governmental bodies, allowing a profile to be produced on an individual's behavior on which decisions, detrimental to an individual, may be taken.

Furthermore, there is an issue over the control of data—information that was altered or removed by the user may in fact be retained and passed to third parties. This danger was highlighted when the controversial social networking site Quechup harvested e-mail addresses from users' e-mail accounts for use in a spamming operation.

Privacy on social networking sites can be undermined by many factors. For example, users may disclose personal information, sites may not take adequate steps to protect user privacy, and third parties frequently use information posted on social networks for a variety of purposes. "For the Net generation, social networking sites have become the preferred forum for social interactions, from posturing and role playing to simply sounding off. However, because such forums are relatively easy to access, posted content can be reviewed by anyone with an interest in the users' personal information".

Privacy Threats:

- Privacy implications associated with online social networking depend on the level of identifiability of the information provided, it's possible recipients, and its possible uses.

- Face Identification

- Demographic data

- It is relatively easy for anyone to gain access to it. By joining the network, hackingthe site, or impersonating a user by stealing his password.

- Stalking to identity theft.

- Personal data is generously provided and limiting privacy preferences are sparinglyused.

- Due to the variety and richness of personal information disclosed in Facebook profiles, their visibility, their public linkages to the members' real identities, and the scope of the network, users may put themselves at risk.

- Building Digital Dossier

Privacy concerns have been found to differ between users according to gender and personality. Women are less likely to publish information that reveals methods of contacting them. Personality measures openness, extraversion, and conscientiousness were found to positively affect the willingness to disclose data, while neuroticism decreases the willingness to disclose personal information.

Many social networks provide an online environment for people to communicate and exchange personal information for dating purposes. Intentions can vary from looking for a one time date, short-term relationships, and long-term relationships.Most of these social networks, just like online dating services, require users to give out certain pieces of information. This usually includes a user's age, gender, location, interests, and perhaps a picture. Releasing very personal information is usually discouraged for safety reasons. This allows other users to search or be searched by some sort of criteria, but at the same time people can maintain a degree of anonymity similar to most online dating services. Online dating sites are similar to social networks in the sense that users create profiles to meet and communicate with others, but their activities on such sites are for the sole purpose of finding a person of interest to date. Social networks do not necessarily have to be for dating; many users simply use it for keeping in touch with friends, and colleagues.

However, an important difference between social networks and online dating services is the fact that online dating sites usually require a fee, where social networks are free. This difference is one of the reasons the online dating industry is seeing a massive decrease in revenue due to many users opting to use social networking services instead. Many popular online dating services such as Match.com, Yahoo Personals, and eHarmony.com are seeing a decrease in users, where social networks like MySpace and Facebook are experiencing an increase in users.One common form of surveillance is to create maps of social networks based on data from social networking sites such as Facebook, MySpace, Twitter as well as from traffic analysis information from phone call records such as those in the NSA call database, and others. These social network "maps" are then data mined to extract useful information such as personal interests, friendships & affiliations, wants, beliefs, thoughts, and activities.

Some people believe that the use of social networking sites is a form of "participatory surveillance", where users of these sites are essentially performing surveillance on themselves, putting detailed personal information on public websites where it can be viewed by corporations and governments. In 2008, about 20% of employers reported using social networking sites to collect personal data on prospective or current employees.

Existing System:

Privacy protection is an important study topic in Mobile social networking. The social networking platforms are comprehensive of the mobile environment, users need more widespread privacy-preservation for the reason that they are new with the neighbors in surrounding area who may store, and compare their personal information at different time periods and locations. Once the private data is associated to the location information, the actions of users will be totally revealed to the general public.

To overcome the privacy violation in OSNs and MSNs, many privacy enhancing techniques have been adopted into the OSN & MSN applications.
The existing work could model and analyze access control requirements with respect to collaborative authorization management of shared data in OSNs. The need of joint management for data sharing, especially photo sharing, in OSNs has been recognized by the recent work provided a solution for collective privacy management in OSNs. Their work considered access control policies of a content that is co-owned by multiple users in an OSN, such that each co-owner may separately specify her/his own privacy preference for the shared content.

Threats in Online & Mobile Social Networks:

1. Digital record aggregation: Profiles on OSNs & MSNs can be downloaded and stored by third parties, creating a digital record of private data.

2. Secondary data collection: Information knowingly revealed in a profile. Various researches propose that such data is being used to significant monetary gain.

3. Face recognition: User-provided digital images are a very popular part of profiles on MSNs. The picture is, in effect, a binary identifier for the user, allowing linking across profiles.

4. Difficulty of complete account deletion: Users aspiring to remove accounts from OSNs & MSNs discover that it is more or less not possible to delete secondary information linked to their profile such as public comments on other profiles.

5. Difficult to guard from malicious users who are snooping about the personal information of other users.

6. Difficult to safeguard from neighbors in mobile environment who may snoop, store, and compare their personal information.

7. The Internet stores an everlasting record of the conversation which can be tracked.

8. Using non-secure passwords might perhaps be without difficulty guessed by cyber criminals and compromise your OSN & MSN account to spam your contacts.

Proposed System:

We distinguish three types of privacy problems that researchers in computer science tackle. The first approach addresses the "surveillance problem" that arises when the personal information and social interactions of OSN users are leveraged by governments and service providers.

The second approach addresses those problems that emerge through the necessary renegotiation of boundaries as social interactions get mediated by OSN services, in short called "social privacy". The third approach addresses problems related to users losing control and oversight over the collection and processing of their information in OSNs, also known as "institutional privacy".

MODULE DESCRIPTION:

Number of Modules:

After careful analysis the system has been identified to have the following modules:

1.The Social Privacy Module

2.Surveillance Module

3.Institutional Privacy Module

4.Approach To Privacy As Protection Module

1.The Social Privacy Module:

Social privacy relates to the concerns that users raise and to the harms that they experience when technologically mediated communications disrupt social boundaries. The users are thus "consumers" of these services. They spend time in these (semi-)public spaces in order to socialize with family and friends, get access to information and discussions, and to expand matters of the heart as well as those of belonging. That these activities are made public to 'friends' or a greater audience is seen as a crucial component of OSNs. In Access Control, solutions that employ methods from user modeling aim to develop "meaningful" privacy settings that are intuitive to use, and that cater to users' information management needs.

2.Surveillance Module:

With respect to surveillance, the design of PETs starts from the premise that potentially adversarial entities operate or monitor OSNs. These have an interest in getting hold of as much user information as possible, including user-generated content (e.g., posts, pictures, private messages) as well as interaction and behavioral data (e.g., list of friends, pages browsed, 'likes'). Once an adversarial entity has acquired user information, it may use it in unforeseen ways – and possibly to the disadvantage of the individuals associated with the data.

3.Institutional Privacy Module:

The way in which personal control and institutional transparency requirements, as defined through legislation, are implemented has an impact on both surveillance and social privacy problems, and vice versa. institutional privacy studies ways of improving organizational data management practices for compliance, e.g., by developing mechanisms for information flow control and accountability in the back end. The challenges identified in this paper with integrating surveillance and social privacy are also likely to occur in relation to institutional privacy, given fundamental differences in assumptions and research methods.

4.Approach To Privacy As Protection Module:

The goal of PETs ("Privacy Enhancing Technologies") in the context of OSNs is to enable individuals to engage with others, share, access and publish information online, free from surveillance and interference. Ideally, only information that a user explicitly shares is available to her intended recipients, while the disclosure of any other information to any other parties is prevented. Furthermore, PETs aim to enhance the ability of a user to publish and access information on OSNs by providing her with means to circumvent censorship.

Conclusion:

In this paper, I studied the aspect of surveillance and Privacy Protection. It is important to see the inter dependence and correlation of Surveillance and Privacy Protection, rather than work them as if they are two completely different issues.

REFERENCES :

[1]Seda Gurses and Claudia Diaz, Two tales of privacy in online social networks IEEE Security & Privacy 11(3):29-37,May/June 2013.

[2].F. Beato, M.Kohlweiss , and K.Wouters. Scramble! your social network data. In Privacy Enhancing Technologies Symposium, PETS 2011, volume 6794 of LNCS, pages 211–225. Springer, 2011.

[3] J. Anderson, C. Diaz, J. Bonneau, and F. Stajano. Privacy-Enabling Social Networking over Untrusted Networks. In ACM Workshop on Online Social Networks (WOSN), pages 1–6. ACM, 2009.

[4] E. De Cristofaro, C. Soriente, G. Tsudik, and A. Williams. Humming- bird: Privacy at the time of twiter. In IEEE Symposium on Security and Privacy, pages 285–299. IEEE Computer Society, 2012.

[5] A. Cutillo, R. Molva, and T. Strufe. Safebook: A privacy-preserving online social network leveraging on real-life trust. Communications Magazine, 47(12):94–101, 2009.

[6] Deirdre K. Mulligan and Jennifer King. Bridging the gap between privacy and design. Journal of Constitutional Law, 14(4):989 – 1034, 2012.

[7] Leysia Palen and Paul Dourish. Unpacking ”privacy” for a networked world. In CHI ’03, pages 129 – 136, 2003.

[8] Kate Raynes-Goldie. Privacy in the Age of Facebook: Discourse, Architecture, Consequences. PhD thesis, Curtin University, 2012.

[9] Rula Sayaf and Dave Clarke. Access control models for online social lnet works. In Social Network Engineering for Secure Web Data and Services. IGI - Global, (in print) 2012.

[10] Fred Stutzman and Woodrow Hartzog. Boundary regulation in social media. In CSCW, 2012.

[11] Irma Van Der Ploeg. Keys To Privacy. Translations of “the privacy problem” in Information Technologies, pages 15–36. Maastricht: Shaker, 2005.

[12] Deirdre K. Mulligan and Jennifer King. Bridging the gap between privacy and design. Journal of Constitutional Law, 14(4):989 – 1034, 2012.

[13] Leysia Palen and Paul Dourish. Unpacking ”privacy” for a networked world. InCHI ’03, pages 129 – 136, 2003.

Volume No:1, Issue No:1 (June-2015)

International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

An Innovative Method That Distinguishes Between Botnet Traffic and Legitimate Traffic in Internet Chats

E. likith
B.Tech Student,
Depatment of CSE,
TKR College of Engineering & Technology.

K. Latha
B.Tech Student,
Depatment of CSE,
TKR College of Engineering & Technology.

A.Pramod Reddy
Associate Professor,
Depatment of CSE,
TKR College of Engineering & Technology.

Abstract:

A botnet is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks. This can be as mundane as keeping control of an Internet Relay Chat (IRC) channel, or it could be used to send spam email or participate in distributed denial-of-service attacks. The word botnet is a combination of the words robot and network. The term is usually used with a negative or malicious connotation.Peer-to-Peer botnets are legally taken by botmasters for the quick recovery against taking down effortsof the system. But it's a harder one for the botmasters, because modern botnets are hidden and performing maliciousactivities it makes the process inefficient. Additionally because of sudden growth of the network traffic there was anability to enlarge the malicious activities of the system. In this paper, the hidden P2P botnets are identified usingbotmasters. Our system first identifies the system which is all engaged in p2p communications. Then it analysis thebehavioral characteristics of identifying P2P and it finds the difference between P2P botnet traffic and legal p2p traffic. By doing this our scalability of our system increases. Alternatively it also increases the detection accuracy as well asscalability of our system.

Keywords: Botnets, Traffic, Legitimate traffic, P2P, Botmaster.

Introduction:

A botnet (also known as a zombie army) is a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet. Any such computer is referred to as a zombie - in effect, a computer "robot" or "bot" that serves the wishes of some master spam or virus originator. Most computers compromised in this way are home-based. According to a report from Russian-based Kaspersky Labs, botnets -- not spam, viruses, or worms -- currently pose the biggest threat to the Internet. A report from Symantec came to a similar conclusion.

Types of botnets:

Legal botnets:

The term botnet is widely used when several IRC bots have been linked and may possibly set channel modes on other bots and users while keeping IRC channels free from unwanted users. This is where the term is originally from, since the first illegal botnets were similar to legal botnets. A common bot used to set up botnets on IRC is eggdrop.

Illegal botnets:

Botnets sometimes compromise computers whose security defenses have been breached and control conceded to a third party. Each such compromised device, known as a "bot", is created when a computer is penetrated by software from a malware (malicious software) distribution. The controller of a botnet is able to direct the activities of these compromised computers through communication channels formed by standards-based network protocols such as IRC and Hypertext Transfer Protocol (HTTP). A botnet's originator (known as a "bot herder" or "bot master") can control the group remotely, usually through IRC, and often for criminal purposes. This server is known as the command-and-control (C&C) server. Though rare, more experienced botnet operators program command protocols from scratch. These protocols include a server program, a client program for operation, and the program that embeds the client on the victim's machine. These communicate over a network, using a unique encryption scheme for stealth and protection against detection or intrusion into the botnet.[citation needed]A bot typically runs hidden and uses a covert channel (e.g. the RFC 1459 (IRC) standard, Twitter, or IM) to communicate with its C&C server. Generally, the perpetrator has compromised multiple systems using various tools (exploits, buffer overflows, as well as others; see also RPC). Newer bots can automatically scan their environment and propagate themselves using vulnerabilities and weak passwords. Generally, the more vulnerabilities a bot can scan and propagate through, the more valuable it becomes to a botnet controller community.

The process of stealing computing resources as a result of a system being joined to a "botnet" is sometimes referred to as "scrumping."Botnet servers are typically redundant, linked for greater redundancy so as to reduce the threat of a takedown. Actual botnet communities usually consist of one or several controllers that rarely have highly developed command hierarchies; they rely on individual peer-to-peer relationships.

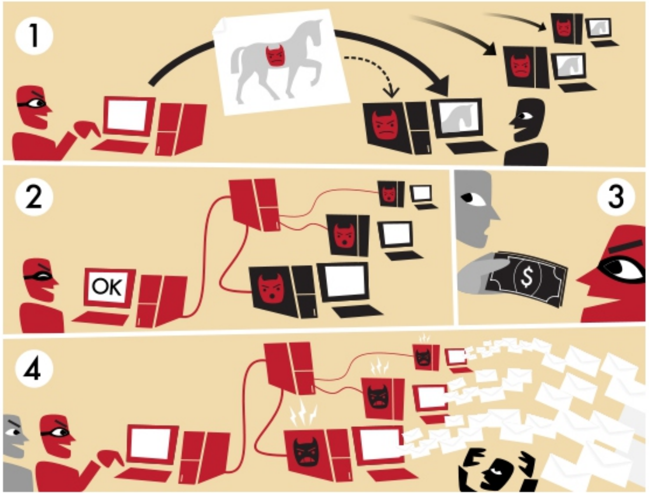
Botnet architecture evolved over time, and not all botnets exhibit the same topology for command and control. Advanced topology is more resilient to shutdown, enumeration or discovery. However, some topologies limit the marketability of the botnet to third parties.[6] Typical botnet topologies are Star, Multi-server, Hierarchical and Random.This example illustrates how a botnet is created and used to send email spam.

- A botnet operator sends out viruses or worms, infecting ordinary users' computers, whose payload is a malicious application—the bot.
- The bot on the infected PC logs into a particular C&C server.

- A spammer purchases the services of the botnet from the operator.

- The spammer provides the spam messages to the operator, who instructs the compromised machines via the control panel on the web server, causing them to send out spam messages.

How a Botnet works:



Types of attacks:

- In distributed denial-of-service attacks, multiple systems submit as many requests as possible to a single Internet computer or service, overloading it and preventing it from servicing legitimate requests. An example is an attack on a victim's phone number. The victim is bombarded with phone calls by the bots, attempting to connect to the Internet.

- Adware advertises a commercial offering actively and without the user's permission or awareness, for example by replacing banner ads on web pages with those of another advertiser.

- Spyware is software which sends information to its creators about a user's activities – typically passwords, credit card numbers and other information that can be sold on the black market. Compromised machines that are located within a corporate network can be worth more to the bot herder, as they can often gain access to confidential corporate information. Several targeted attacks on large corporations aimed to steal sensitive information, such as the Aurora botnet.

- E-mail spam are e-mail messages disguised as messages from people, but are either advertising, annoying, or malicious.

- Click fraud occurs when the user's computer visits websites without the user's awareness to create false web traffic for personal or commercial gain.

- Fast flux is a DNS technique used by botnets to hide phishing and malware delivery sites behind an ever-changing network of compromised hosts acting as proxies.

- Brute-forcing remote machines services such as FTP, SMTP and SSH.

- Worms. The botnet focuses on recruiting other hosts.

- Scareware is software that is marketed by creating fear in users. Once installed, it can install malware and recruit the host into a botnet. For example users can be induced to buy a rogue anti-virus to regain access to their computer.

- Exploiting systems by observing users playing online games such as poker and see the players' cards.

PROPOSED SYSTEM:

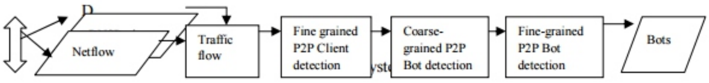
In this paper a novel scalable botnet detection system has been proposed. This detection system is capable of detectingstealthy P2P botnets whose malicious activities may not be observable in the network traffic.Our system aims todetect stealthy P2P botnets even if P2P botnet traffic is overlapped with the traffic generated by legal P2P applicationsrunning on the same compromised host.

Our system identifies P2P bots within a monitored network by detecting theC&C communication patterns that characterize P2P botnets. The high scalability of the system can be achieved byusing the following techniques.1. P2P traffic profiling algorithm that is used to built the statistical fingerprints for various P2P applications.2. A flow-clustering based analysis approach to identify host that engaged in P2P communications.

3. A scalable design based on an efficient detection algorithms and parallelized computation.

4. A prototype system based on real world network traffic which demonstrated high detection accuracy. The new model eradicates the necessity of keeping failed connections. Clustering based client detection algorithmenhances the efficiency of the model. The system is parallelized to boost scalability and efficiency. The proposedsystem is effective over a large range of parameter values.

System Design:


D
Netflow
Traffic flow
Fine grained P2P Client detection
yste
Coarse-grained P2P Bot detection
Fine-grained P2P Bot detection
Bots

A P2P botnet depends on P2P protocol to create transmission through C&C channel with botmasters. A P2P bots havea common network traffic patterns that is used to evolve P2P client applications as well as legal applications. It dividesin two phases (1) In first phase, Its aims is to detect all the network traffic which involved in peer-to-peer communications.

In figure we inspect the network flow at the edge and filter it to discard the flow which should becreated unexpectedly by peer-to-peer applications. From that we can analysis the network traffic and flow created bypeer-to-peer clients. (2) In second phase, our system will examine the network traffic generated by both legal P2Pclients and P2P bots. Then we explore the active time of the peer-to-peer client and recognize it as candidate P2P botand if there is a continuous change in host. We further analyze it by detecting 2 candidates P2P bots.

Finding out Peer-to-Peer Client:
A Filter:

Filter component is used to filter the network traffic that is unrelated to P2P communications. This can be achieved byanalyzing DNS traffic. P2P clients contact their peers by looking up IPs from a routing table for the overlay networkrather than resolving a domain name. Most non P2P applications often connect to a destination address resulting fromdomain name resolution. This simple filter can eliminate a very large percentage of non P2P traffic and helps inretaining P2P communication.

B Peer-to-Peer Detector:

Client detector helps in detecting P2P clients by analyzing the remaining network traffic .For each host within themonitored network we identify two flow sets which contains flows related to sucessful outgoing TCP and UDPconnections.

TCP connection is considered successful if SYN,SYN/ACK,ACK I handshake is available.UDP connection is considered successful if there is at least one request and a consequent response packet is found. Inorder to detect P2P clients we first consider the fact that each P2P client frequently exchanges control messages withother peers. Even though the characteristics of these messages such as size and the frequency of the exchanged packetsare same ,they vary depending upon the P2P protocol and network in use. If two network flows are generated by thesame P2P applications they carry the same control messages. In addition P2P client exchanges the control messageswith large number of peers that is distributed in different networks. The destination IP addresses of network flows that carry these control messages will spread across a large number of networks where each network can be represented by its BGP prefix.

Finding Peer-to-Peer Bots:
Coarse-Grained Detection of P2P Bots:

Since bots are malicious programs used to perform profitable malicious activities, they represent valuable assets for the botmasters, who will intuitively try to maximize utilization of bots. This is particularly true for P2P bots because in order to have a functional overlay network, a sufficient number of peers needs to be always online. In other words the active time of the bots should be comparable with the active time of the underlying compromised system. If this was not the case the botnet overlay network would risk degenerating into a number of disconnected subnetworks due to the short lifetime of each single node. In contrast the active time of the legitimate P2P applications determined by users, which is likely to be transient.

Fine-Grained Detection of P2P Bots:

The objective of this component is to identify P2P bots from all persistent P2P clients. We leverage one feature; the overlap of peers connected by two P2P bots belonging to the same P2P botnets is much larger than that contacted by two clients in the same legitimate P2P network. Assume two hosts in the monitored network are running the same legitimate P2P file sharing application (e.g., Emule). Users of these two P2P clients will most likely have uncorrelated usage patterns. It is reasonable to assume that in the general case the two users will search for and download different contents(e.g., different media files or documents)from the P2P network. This translates into a divergence between the set of IP addresses contacted by hosts.

Conclusion:

The computers that form a botnet can be programmed to redirect transmissions to a specific computer, such as a Web site that can be closed down by having to handle too much traffic - a distributed denial-of-service (DDoS) attack - or, in the case of spam distribution, to many computers. In this paper we proposed a novel scalable P2P botnet detection system that is able to identify stealthy P2P botnets.

To perform this task statistical fingerprints of P2P communications have been derived to detect P2P clients and furtherdistinguish between those that are part of legitimate P2P networks and P2P bots. The results shows that the proposedsystem accomplishes high accuracy on detecting stealthy P2P bots and great scalability.

References:

[1] Junjie Zhang, Roberto Perdisci, Wenke Lee, Xiapu Luo, and Unum Sarfraz, Building a Scalable System for Stealthy P2P-Botnet Detection, EEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 1, JANUARY 2014.

[2] A. Ramachandran, N. Feamster, and S. Vempala, " Filtering spam with behavioral blacklisting", In ACM CCS, 2007.

[3] M. A. Rajab, J. Zarfoss, F. Monrose, and A. Terzis, " A multifaceted approach to understanding the botnet phenomenon",In IMC, 2006.

[4] D. Dittrich and K. E. Himma, "Active Response to Computer Intrusions,"in The Handbook of Information Security, edited by H. Bidgoli(Wiley,New York, 2005).

[5] Y. Zhao, Y.Xie, F.Yu and Y.Yu, "Botgraph : Large scale spamming botnet detection", in Proc. 6th USENIX NSDI, 2009, pp 1-14.

[6] G.Gu ,R.Perdisci, J.Zhang and W.Lee, "Botminer: Clustering analysis of network traffic for protocol and structure independent botnet detection",in Proc. UNISEX security, 2008, pp.139-154.

[7] M. A. Rajab, J. Zarfoss, F. Monrose, and A. Terzis, " A multifaceted approach to understanding the botnet phenomenon"In IMC, 2006.

[8] D. S. Anderson, C. Fleizach, S. Savage, and G. M. Voelker. Spamscatter: Characterizing internet scam hosting infrastructure. In USENIX SecuritySymposium, 2007

[9] Y. Xie, F. Yu, K. Achan, R. Panigrahy, G. Hulten, and Osipkov. Spamming botnets: Signatures and characteristics.In SIGCOMM, 2008.

[10] Y. Yu, M. Isard, D. Fetterly, M. Budiu, U. Erlingsson,P. K. Gunda, and J. Currey, " DryadLINQ: A system forgeneral-purpose distributed data-parallel computing using a high-level language", In OSDI, 2008.

[11] G.Bartlett, J.Heidemenn and J. Pepin, "Estimating P2P traffic volume at USC",USA,Tech. Rep. ISI-TR-2007

About Author's:

E. likith
B.Tech Student,
Depatment of CSE,
TKR College of Engineering & Technology.

K. Latha
B.Tech Student,
Depatment of CSE,
TKR College of Engineering & Technology.

A.Pramod Reddy
Associate Professor,
Depatment of CSE,
TKR College of Engineering & Technology.

Volume No:1, Issue No:1 (June-2015)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

Protecting Privacy While Enforcing Attribute Based ACPs in Cloud Computing

Pinninti Sushma
B.Tech Student,
Depatment of CSE,
TKR College of Engineering &
Technology.

Dr.A.Suresh Rao, MTech, Ph.D,
Professor &HoD,
Depatment of CSE,
TKR College of Engineering &
Technology.

B.Jaya Lakshmi
Assistant Professor,
Depatment of CSE,
TKR College of Engineering &
Technology.

Abstract:

Cloud computing is typically defined as a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. In cloud computing, the word cloud (also phrased as "the cloud") is used as a metaphor for "the Internet," so the phrase cloud computing means "a type of Internet-based computing," where different services — such as servers, storage and applications — are delivered to an organization's computers and devices through the Internet.To maintain the shared data confidential against untrusted cloud service providers (CSPs), a natural way is to store only the encrypted data in a cloud.

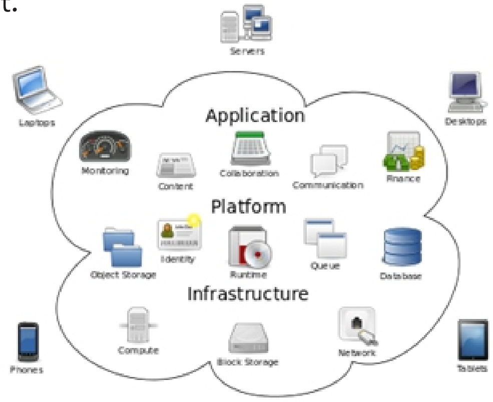
The major problems of this approach include establishing Decomposing Access Control Polices, delegated access control for the encrypted data, proof of ownership allow storage server to check a user data ownership based on hash value and the access rights from users when they are no longer authorized to access the encrypted data. In the proposed approach the privacy of users is protected while enforcing attribute based ACPs and utilizing the two layer of encryption reduce the overhead at Owner, opposed to unauthorized access to data and to any data leak during sharing process, providing levels of access control verification.

Keywords:

Privacy, Cloud computing, data sharing, policy decomposition, privacy preserving, access control, Two layer encryption

Introduction:

In a cloud computing system, there's a significant workload shift. Local computers no longer have to do all the heavy lifting when it comes to running applications. The network of computers that make up the cloud handles them instead. Hardware and software demands on the user's side decrease. The only thing the user's computer needs to be able to run is the cloud computing system's interface software, which can be as simple as a Web browser, and the cloud's network takes care of the rest.



Cloud Computing

The National Institute of Standards and Technology's definition of cloud computing identifies "five essential characteristics":On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations). Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear unlimited and can be appropriated in any quantity at any time.Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Related Work:

Mohamed Nabeel and Elisa Bertino, proposed a paper [1] "Privacy preserving delegated access control in public cloud", these afford efficient group key management scheme that supports expressive ACPs. It assures the confidentiality of the data and preserves the privacy of users from the cloud while delegating most of the access control enforcement to the cloud. Here two layer encryption is performed, one by data owner and another one by cloud. Under our approach, the data owner performs a coarse-grained encryption, where cloud performs a fine-grained encryption on top of the owner encrypted data. A major issue is how to decompose access control policies (ACPs) such that the two layer encryption can be performed. Our approach is based on a privacy preserving attribute based key management scheme that protect the privacy of users while enforcing attribute based ACPs.

Here decomposing the ACPs and utilize the two layer of encryption decrease the transparency at the Owner. MohamadNabeel Dept. of Computer Science., Purdue Univ., West Lafayette, IN, USA, proposed a paper [2] "Privacy preserving delegated access control in the storage as a service model". Here a new approach for delegating privacypreserving fine-grained access enforcement to the cloud. The approach is based on a recent key management scheme that allows users whose attributes satisfy a certain policy to derive the data encryption keys only for the content they are allowed to access from the cloud. His approach preserves the confidentiality of the data and the user privacy from the cloud, where delegating most of the access control enforcement to the cloud.

Additionally, in order to reduce the cost of re-encryption required whenever the access control policies changes, these approach uses incremental encryption techniques.Elisa Bertino, Mohamed Nabeel proposed a paper [5] "Towards attribute based group key management". Attribute based system permit fine-grained access control among a group of users each identified by a set of attributes. A protected collaborative applications need such flexible attribute based systems for managing and distributing group keys. These system able to support any monotonic access control policy over a set of attributes. When the group changes, the rekeying operations do not affect the private information of existing group members and thus our schemes eliminate the need of establishing expensive private communication channels.NesrineKaaniche, Maryline Laurent proposed a paper [6] "A Secure Client Side Deduplication Scheme in Cloud Storage Environments", here a new client-side deduplication scheme for securely storing and sharing outsourced data via the public cloud that towards the security and privacy of the public cloud environments. Here originality of proposal system is twofold. First, it ensures better confidentiality towards unauthorized users. Therefore every client compute a per data key to encrypt the data that he intends to store in the cloud. As such, the data access is managed by the data owner. Second, by integrate access privileges in metadata file, an authorized user can decode an encrypted file only with his private key. These solution is also shown to be resistant to unauthorized access to data and to any data disclosure during sharing procedure, given that two levels of access control verification.

EXISTING SYSTEM:

Many organizations have today ACPs regulating which users can access which data; these ACPs are often expressed in terms of the properties of the users, referred to as identity attributes, using access control languages such as XACML. Such an approach, referred to as attribute based access control (ABAC), supports fine-grained access control which is crucial for high-assurance data security and privacy. Supporting ABAC over encrypted data is a critical requirement in order to utilize cloud storage services for selective data sharing among different users. Notice that often user identity attributes encode private information and should thus is strongly protected from the cloud, very much as the data themselves.

Approaches based on encryption have been proposed for fine-grained access control over encrypted data. Those approaches group data items based on ACPs and encrypt each group with a different symmetric key. Users then are given only the keys for the data items they are allowed to access. Extensions to reduce the number of keys that need to be distributed to the users have been proposed exploiting hierarchical and other relationships among data items

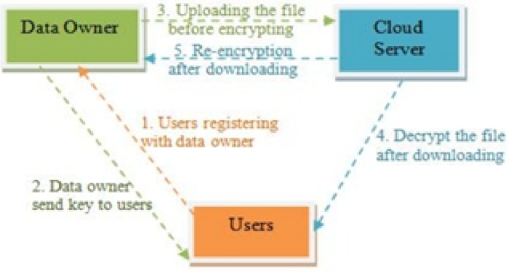
DISADVANTAGES OF EXISTING SYSTEM:

- As the data owner does not keep a copy of the data, when ever user dynamics changes, the data owner needs to download and decrypt the data, re-encrypt it with the new keys, and upload the encrypted data. The user dynamics refers to the operation of adding or revoking users. Notice also that this process must be applied to all the data items encrypted with the same key. This is inefficient when the data set to be re-encrypted is large.

- In order to issue the new keys to the users, the data owner needs to establish private communication channels with the users.

- The privacy of the identity attributes of the users is not taken into account. Therefore the cloud can learn sensitive information about the users and their organization.

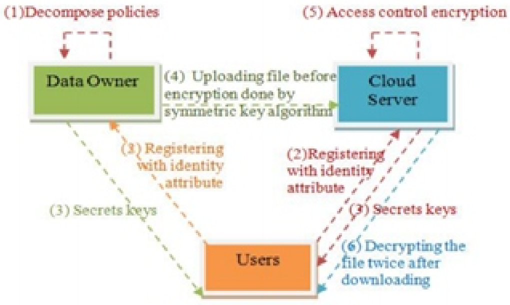
- They are either unable or inefficient in supporting fine-grained ABAC policies.


Data Owner
3. Uploading the file before encrypting
5. Re-encryption after downloading
Cloud Server
1. Users registering with data owner
4. Decrypt the file after downloading
2. Data owner send key to users
Users

Traditional Encryption Approach

PROPOSED SYSTEM:

In this paper, we propose a new approach to address this shortcoming. The approach is based on two layers of encryption applied to each data item uploaded to the cloud. Under this approach, referred to as two layer encryption (TLE), the data owner performs a coarse grained encryption over the data in order to assure the confidentiality of the data from the cloud. Then the cloud performs fine grained encryption over the encrypted data provided by the data owner based on the ACPs provided by the data owner. It should be noted that the idea of two layer encryption is not new. However, the way we perform coarse and fine grained encryption is novel and provides a better solution than existing solutions based on two layers of encryption. We elaborate in details on the differences between our approach and existing solutions in the related work section.


(1)Decompose policies
(5) Access control encryption
Data Owner
(4) Uploading file before encryption done by symmetric key algorithm
Cloud Server
(3) Registering with identity attribute
(2)Registering with identity attribute
(3) Secrets keys
(3) Secrets keys
Users
(6) Decrypting the file twice after downloading

Hybrid Encryption Approach

A challenging issue in the TLE approach is how to decompose the ACPs so that fine-grained ABAC enforcement can be delegated to the cloud while at the same time the privacy of the identity attributes of the users and confidentiality of the data are assured. In order to delegate as much access control enforcement as possible to the cloud, one needs to decompose the ACPs such that the data owner manages minimum number of attribute conditions in those ACPs that assures the confidentiality of data from the cloud. Each ACP should be decomposed to two sub ACPs such that the conjunction of the two sub ACPs result in the original ACP. The two layer encryption should be performed such that the data owner first encrypts the data based on one set of sub ACPs and the cloud re-encrypts the encrypted data using the other set of ACPs. The two encryptions together enforce the ACP as users should perform two decryptions to access the data.

ADVANTAGES OF PROPOSED SYSTEM:

The TLE approach has many advantages.

- When user dynamics changes, only the outer layer of the encryption needs to be updated. Since the outer layer encryption is performed at the cloud, no data transmission is required between the data owner and the cloud.

- Further, both the data owner and the cloud service utilize a broadcast key management whereby the actual keys do not need to be distributed to the users.

- Instead, users are given one or more secrets which allow them to derive the actual symmetric keys for decrypting the data.

TWO LAYER ENCRYPTION METHOD:

Identity token providence: IdPs issue identity tokens to Users based on their identity attributes.Policy decomposition: The Owner decomposes each ACP into at most two sub ACPs such that the Owner enforces the minimum number of attributes to assure confidentiality of data from the Cloud. It is important to make sure that the decomposed ACPs are consistent so that the sub ACPs together moves the original ACPs. The Owner enforces the confidentiality related sub ACPs and the Cloud enforces the remaining sub ACPs.Identity token registration: Users register their identity tokens in order to obtain secrets to decrypt the data that they are allowed to access. Users register only those identity tokens related to the Owner's sub ACPs and register the remaining identity tokens with the Cloud in a privacy preserving manner. It should be noted that the Cloud does not learn the identity attributes of Users during this phase.

Data encryption and uploading: The Owner encrypts the data based on the Owner's sub ACPs in order to hide the content from the Cloud and then uploads them along with the public information generated by the keygen algorithm and the remaining sub ACPs to the Cloud. It in turn allows data encryption based on the keys generated using its own algorithm. Note that the Keys at the Cloud takes the secrets issued to Users and the sub ACPs given by the Owner into consideration to generate keys. Data downloading and decryption: Users download encrypted data from the Cloud and decrypt the data using the derived keys. The users decrypt the data twice.

CONCLUSION:

In this paper, we present a unique method for privacy preserving of data storage in multi-cloud environment. It also provides several advancements in cloud computing due to its technical capabilities. The feature work may also involves load-balancing in multi-cloud environment for maximum storage and accuracy for various users. Cloud computing is a growing paradigm as an enabling technology to deliver on-demand and elastic storage and computing capabilities, while removing the ownership need for hardware. But several privacy and security act demand strong protection of the cloud users, which in turn increases the complexity to develop privacy-preserving cloud services. The privacy preserving using delegated access control in multi-cloud delivers the critical capabilities required for a robust, cost-effective, and secure cloud security implementation.

References:

1. M. Nabeel and E. Bertino, “Privacy preserving delegated access control in public cloud,” in IEEE Transactions on Knowledge and Data Engineering, 2014.

2. M. Nabeel and E. Bertino, “Privacy preserving delegated access control in the storage as a service model” in IEEE International Conference on Information Reuse and Integration (IRI), 2012.

3. M. Nabeel and E. Bertino, “Privacy preserving policy based content sharing in public clouds,“In IEEE Transactions on Knowledge and Data Engineering, 2012.

4. M. Nabeel, E. Bertino, M. Kantarcioglu, and B. M. Thuraisingham, “Towards privacy preserving access control in the cloud,” in Proceedings of the 7th International Conference on Collaborative Computing: Networking, Applications and Work sharing, ser. Collaborate Com ’11, 2011,pp. 172–180.

5. M. Nabeel and E. Bertino, “Towards attribute based group key management,” in Proceedings of the 18th ACM conference on Computer and communications security, Chicago, Illinois, USA, 2011.

6. NesrineKaaniche, Maryline Laurent,” A Secure Client Side Deduplication Scheme in Cloud Storage Environments” 6th International Conference on new Technologies, Mobility and Security year 2014.

7. D. Harnik, B. Pinkas, and A. Shulman-Peleg. Side channels in cloud services: Deduplication in cloud storage. IEEE Security And Privacy, 8(6):40–47, 2010.

8. A.Fiat and M. Naor, “Broadcast Encryption,” Proc. 13th Ann. Int’l Cryptology Conf. Advances in Cryptology (CRYPTO ’93), pp. 480-491, 1994.

9. D. Hankerson, A. J. Menezes, and S. Vanstone. Guide to Elliptic Curve Cryptography. Springer-Verlag New York, Inc., Secaucus, NJ, USA,2003.

10. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-Policy Attri-bute-Based Encryption,” Proc. IEEE Symp. Security and Privacy (SP ’07), pp.321-334, 2007.

11. E. Bertino and E. Ferrari, “Secure and Selective Dissemination of XML Documents,” ACM Trans. Information and System Security, vol. 5, no.3, pp. 290-321, 2002.

12. J. Camenisch, M. Dubovitskaya, and G. Neven, “Oblivious Trans-fer with Access Control,” Proc. 16th ACM Conf. Computer and Comm.Security (CCS ’09), pp. 131-140, 2009.

13. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,” Proc. 13thACM Conf. Computer and Comm. Security (CCS ’06), PP 89-98, 2006.

14. J. Xu, E.-C.Chang, and J. Zhou. Weak leakage-resilient client-side deduplication of encrypted data in cloud storage. In Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security, ASIA CCS ’13, pages 195–206, New York, NY, USA, 2013. ACM.

15. R. C. Merkle. A digital signature based on a conventional encryption function. In A Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology, CRYPTO ’87, pages 369–378, London, UK, UK, 1988. Springer-Verlag.

16. R. C. Merkle. A digital signature based on a conventional encryption function. In A Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology, CRYPTO ’87, pages 369–378, London, UK, UK, 1988. Springer-Verlag.

17. SmithaSundareswaran, Anna C. Squicciarini, Member, IEEE, and Dan Lin, “Ensuring Distributed Accountability for Data Sharing in the Cloud” March 2012.

18. Junzuo Lai, Robert H. Deng, Chaowen Guan, and JianWeng “Attribute- Based Encryption with Verifiable Outsourced Decryption” 2013.

Volume No:1, Issue No:1 (June-2015)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

A Novel Design of Effective Security for Data Communication by Designing Standard Algorithm for Encryption and Decryption

Baddam Mounika Reddy
Masters in Embedded Systems,
Department of Electronics and
Communication Engineering,
Stanley College of Engineering and
Technology for Women, Hyderabad,India.

V. Sudarshini Kataksham
Asst Professor,
Department of Electronics and
Communication Engineering,
Stanley College of Engineering and
Technology for Women, Hyderabad,India.

Abstract:

Data security is protecting data, from destructive forces, and from the unwanted actions of unauthorized users. Data Security is primary concern for every communication system. There are many ways to provide security to data that is being communicated. In this paper the proposed technique is data can be transmitted to and received from remote Zigbee communication device. However, what if the security is assured irrespective of the hackers or from the noise. This Paper describes a design of effective security for data communication by designing standard algorithm for encryption and decryption.

Keywords:

Encryption,Security,ARM,Wireless Communication, Zigbee.

I. INTRODUCTION:

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Wireless communication offers the benefits of low cost, rapid deployment, shared communication medium, and mobility; at the same time, it causes many security and privacy challenges .Zigbee is a PAN technology based on the IEEE 802.15.4 standard. Unlike Bluetooth or wireless USB devices, Zigbee devices have the ability to form a mesh network between nodes. Meshing is a type of daisy chaining from one device to another. This technique allows the short range of an individual node to be expanded and multiplied, covering a much larger area.The source information is generated by PS2 Keyboard and this will be encrypted and is sent to destination through Zigbee modules. The receiving system will check the data according to a specific algorithm and displays on the LCD.The proposed technique is built around the controller in the transmitter and receiver section. The controller provides all the functionality of the display and wireless control. It also takes care of creating different display effects for given text. Alphanumerical keyboard is interfaced to the transmitter to type the data and transmit. The message can be transmitted to multi point receivers.

After entering the text, the user can disconnect the keyboard. At any time the user can add or remove or alter the text according to his requirement. Whenever the message is transmitted to the receiver section the garbage or junk message will be displayed on the receiver section 16X2 LCD. In order to read the original message the user should press the encryption key which is connected in the receiver sectionHere we can also have the knowledge about the consuming units of the loads connected through the same wireless network.For example if 2 loads (fan, light) are connected and it has consumed 5 units that will be displayed in LCD at the receiver section. So that we cannot only have the data with security but also we can have the knowledge about the loads connected.

II. RELATED WORK:

Volume No:1, Issue No:1 (June-2015)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

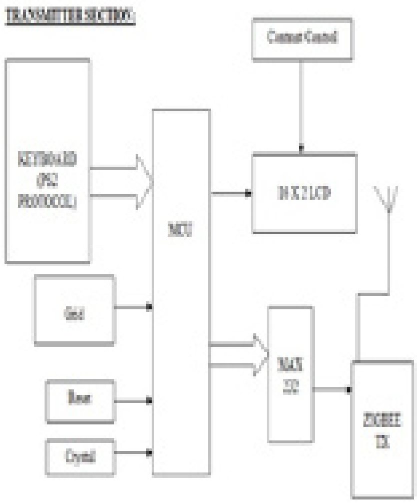


Fig 1: Transmitter Section

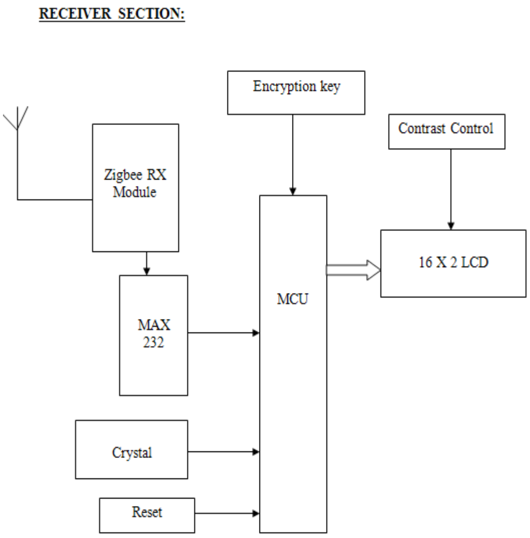


Fig 2: Receiver Section

The LPC2148 are based on a 16/32 bit ARM7TDMI-S™ CPU with real-time emulation and embedded trace support, together with 128/512 kilobytes of embedded high speed flash memory. A 128-bit wide memory interface and unique accelerator architecture enable 32-bit code execution at maximum clock rate. For critical code size applications, the alternative 16-bit Thumb Mode reduces code by more than 30% with minimal performance penalty. With their compact 64 pin package, low power consumption, various 32-bit timers, 4- channel 10-bit ADC, USB PORT,PWM channels and 46 GPIO lines with up to 9 external interrupt pins these microcontrollers are particularly suitable for industrial control, medical systems, access control and point-of-sale.

With a wide range of serial communications interfaces, they are also very well suited for communication gateways, protocol converters and embedded soft modems as well as many other general-purpose applications.

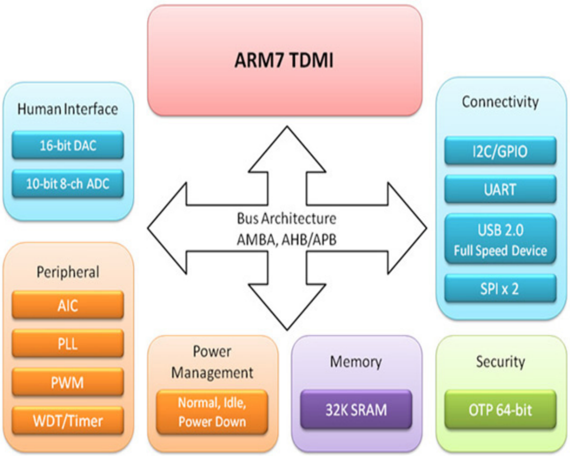


Fig 3 : ARM7 Architecture

ARM7TDMI Processor Core :

- Current low-end ARM core for applications like digital mobile phones

- TDMI

T: Thumb,16-bit compressed instruction set.

D: on-chip Debug support, enabling the processor to halt in response to a debug request

M: enhanced Multiplier, yield a full 64-bit result, high performance

I: Embedded ICE hardware

- Von Neumann architecture

Zigbee:

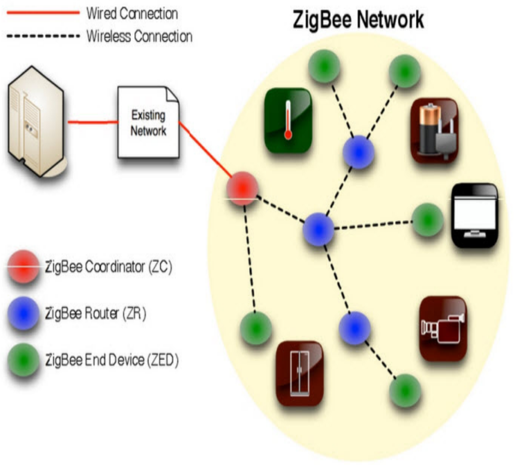


Fig 4 : Zigbee Technology

Zigbee is a PAN technology based on the IEEE 802.15.4 standard. Unlike Bluetooth or wireless USB devices, ZigBee devices have the ability to form a mesh network between nodes. Meshing is a type of daisy chaining from one device to another. This technique allows the short range of an individual node to be expanded and multiplied, covering a much larger area.

Zigbee is the wireless device for transmitting and receiving purpose or simply it called as Transceiver. The range of the Zigbee is covered as 100m. Its range is 10 times better than bluetooth device so it can be more preferable one in wireless device.

Technical Specifications of Zigbee

- Frequency band2.400 - 2.48 GHz
- Number of channels16
- Data rate250 kbps
- Supply voltage1.8 – 3.6 V
- Flash memory128 kB
- RAM8kB
- EEPROMkBOperating
- Temperature-40 — +85 °C

PS/2 (Play Station 2) :

The PS/2 connector is a round shape of 6-pin Mini-DIN connector used for connecting some keyboards and mice to a PC compatible compute r system.

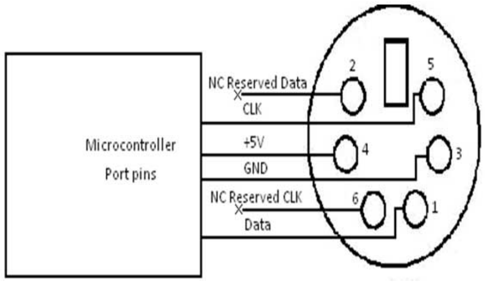


Fig5 :Interfacing PS2 with Micro Controller

Interfacing PS/2:

Fig. 5 shows how to interface PS/2 port to microcontroller.The PS/2 bus includes both clock and data. Both a mouse and keyboard drive the bus with identical signal timings and both use 11-bit words that include a start, stop and odd parity bit. However, the data packets are organized differently for a mouse and keyboard. Furthermore, the keyboard interface allows bidirectional data transfers so the host device can illuminate state LEDs on the Keyboard.

GRID :

The term grid usually refers to a network, and should not be taken to imply a particular physical layout or breadth. Grid may also be used to refer to an entire electrical network, a regional transmission network or may be used to describe a sub network such as a local utility’s transmission grid or distribution grid. The proposed technique uses regulated 3.3V, 500mA power supply. Unregulated 12V DC is used for relay. 7805 three terminal voltage regulator is used for voltage regulation. Bridge type full wave rectifier is used to rectify the ac output of secondary of 230/12V step down transformer.

MAX 232:

Max232 IC is a specialized circuit which makes standard voltages as required by RS232 standards. This IC provides best noise rejection and very reliable against discharges and short circuits.MAX232 IC chips are commonly referred to as line drivers.

III . METHODOLOGY:

The data can be sent to other place with full security. Data need to be given using keyboard and sent using zigbee to other place.The used power (number of units) will also be sent to the receiver. Garbage value is received at other place first.If the encryption key is given then it will be known that the person is authorized. So that the entered data at the other end will be given displayed here .

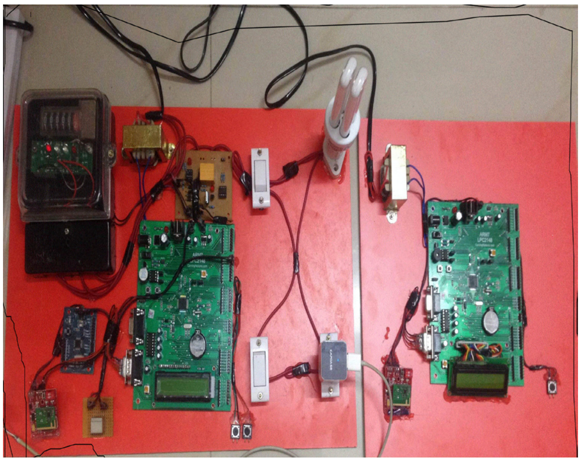


Fig 6 : Demo System

DSE:

In present work, the dynamic secret is employed to design the DSE scheme for grids wireless communication. In this session, we firstly introduce the basic algorithms of dynamic secret; and then present the DSE scheme. The sender and receiver monitor the error retransmission in link layer to synchronously select a group of frames. These frames are hashed into dynamic secret to encrypt the data.

1)Dynamic secret Generation: On the link layer's communication, error retransmission happens unavoidable and randomly at both side of the sender and the receiver. According to Stop-and-Wait (SW) protocol, the sender transmits a frame and waits for the corresponding acknowledgement before sending a new frame. If a frame is only transmitted once and its acknowledgement frame is received in time, this frame is named as one time frame (OTF). After transmitting, the packet 1 is confirmed as an OTF on the sender until the acknowledgement of packet 1 is received; it is confirmed on the receiver until the second packet is received. It will be added into OTF set . Both the transmitted frame (packet 2) and acknowledgement (packet 3) are retransmitted, thus they are not added into OTF set. Once the number of OTF set reaches the threshold, the sender and receiver agree on a uniformly random choice of universal-2 hash functions to com-press into the dynamic secret . Then, the is reset to empty.

2)Encryption/Decryption: When a new dynamic secret is generated, it will be applied to update the encryption key at both sides of communication. This symmetric encryption key is used to encrypt the data at sender and decrypt the cipher at receiver. To reduce the computation consumption, the XOR function is used for encryption and decryption.

DSEScheme for Wireless Communication

Dynamic secret-based encryption (DSE) scheme is designed to secure the wireless communication between the smart devices and control center. The framework of DSE scheme consists of retransmission sequence generation (RSG), DS generation (DSG), and encrypt/decrypt.

1) RSG: This module is applied to monitor the link layer error retransmission.The communication packets which have been retransmitted are marked as "1" and the non-retransmitted packets are marked as "0."The pervious packets are coded as 0/1 sequence , named as retransmission sequence (RS).In DSE, RS is applied to replace the OTF set for dynamic secret generation due to the limitation of computation capability and storage resources.

2) DSG: Once reaches the threshold (length of RS), it would be compressed to a DS in DSG module. Considering the limitation on computation power, the hash functions are recommended in DSG module.are recommended in DSG module.

$$DS(k) = f_{HASH}(\varphi_{L\_RS})$$

3) Encrypt/Decrypt: The new dynamic secret is applied to update the dynamic encryption key (DEK) by

$$DEK(k) = DS(k) \bullet DEK(k-1)$$

Volume No:1, Issue No:1 (June-2015)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

D is generated at both sides of communication synchro-nously. The sender applies it to encrypt the , and the re-ceiver applies it to decrypt the . XOR function, as one of the most light- weight and easy-implementation algorithm, is applied to update the DEK and encrypt/decrypt the data on both sides. If DEK is shorter than the data, is replicated and padded circularly to generatewhose length is equal to the raw data or the raw data or cipher text.

$$\begin{aligned} Data \bullet DEK^{*}(k) &= Cipher \\ Cipher \bullet DEK^{*}(k) &= Data \end{aligned}$$

IV.CONCULSION:

In this paper, a dynamic secret based encryption scheme is designed to secure the wireless communication of SG. To reduce its complexity, the retransmission sequence is proposed to up-date dynamic encryption key, replacing the OTF set;A demo system is developed to investigate the performance of DSE scheme. The numerous experiments reveal that:

1) the DSE scheme can protect the users against eavesdropping by updating the dynamic encryption key with retransmission sequence in communication, even the attackers know the details of DSE scheme and obtain the encryption key at some time; 2) it is a light-weight encryption method with only simple operations, such as MD2 and XOR; 3) it has good compati-bility, which could be integrated with many wireless techniques and applications, such as ZigBee and Modbus.

REFERENCES:

[1]Ting Liu, Member, IEEE, Yang Liu, Yashan Mao, Yao Sun, Xiaohong Guan, Fellow, IEEE,Weibo Gong, Fellow, IEEE, and Sheng Xiao,"A Dyanamic Secret Based Encryption using Smartgrid Wireless Communication", 1949 -3053 © 2013 IEEE.

[2]R. Moghe, F. C. Lambert, and D. Divan, "Smart "Stick-on" sensors for the smart grid," IEEE Trans. Smart Grid, vol. 3, pp. 241–252, 2012.

[3]Federal Energy Regulatory Commission, "Renewables & energy effi-ciency—Generation & efficiency standards" 2011 [Online]. Available: http://www.ferc.gov/market-oversight/othr-mkts/renew.asp

[4]K. Ren, Z. Li, and R. C. Qiu, "Guest editorial cyber, physical, and system security for smart grid," IEEE Trans. Smart Grid, vol. 2, pp. 643–644, 2011.

[5]"The smart grid: An introduction," in DOE's Office of Electricity De-livery and Energy Reliability 2008.

[6]P. Jokar, N. Arianpoo, and V. C. M. Leung, "A survey on security issues in smart grids," Security Commun. Netw., 2012 [Online]. Avail-able: http://http://onlinelibrary.wiley.com/doi/10.1002/sec.559/ab-stract

[7]T. Liu, Y. Gu, D. Wang, Y. Gui, and X. Guan, "A novel method to de-tect bad data injection attack in smart grid," in Proc. IEEE INFOCOM Workshop Commun. Control Smart Energy Syst..

[8]P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," IEEE Security Privacy, vol. 7, pp. 75–77, 2009.

[9]Office of the National Cordination for Smart Grid Interoperability, "NIST framework and roadmap for smart grid interoperability stan-dards," 2010 [Online]. Available: http://www.nist.gov/smartgrid/

[10]Cisco,, "Security for the smart grid," 2009, White Paper [On-line]. Available: http://www.cisco.com/web/strategy/docs/en-ergy/white_paper _c11_539161.pdf

[11]W. Xudong and Y. Ping, "Security framework for wireless communi-cations in smart distribution grid," IEEE Trans. Smart Grid, vol. 2, pp. 809–818, 2011.

[12]P. Jokar, H. Nicanfar, and V. C. M. Leung, "Specifica-tion-based intru-sion detection for home area networks in smart grids," in Proc. 2011 IEEE Int. Conf. Smart Grid Commun. (SmartGridComm), pp. 208–213.

[13]Z. Yichi, W. Lingfeng, S. Weiqing, R. C. Green, and M. Alam, "Arti-ficial immune system based intrusion detection in a distributed hierar-chical network architecture of smart grid," in Proc. 2011 IEEE Power Energy Soc. Gen. Meet., pp. 1–8.

[14]M. M. Fouda, Z. M. Fadlullah, N. Kato, L. Rongxing, and S. Xuemin, "A lightweight message authentication scheme for smart grid commu-nications," IEEE Trans. Smart Grid, vol. 2, pp. 675–685, 2011.

[15]S. Nguyen and C. Rong, "ZigBee security using identity-based cryp-tography autonomic and trusted computing," in Proc. 4th Int. Conf. Autonomic Trusted Comput. (ATC'07), 2007, vol. 4610, Lecture Notes in Computer Science, pp. 3–12.

BIOGRAPHIES:

B.Mounika Reddy

received her B.E degree in Electronic and Communication Engineering from Stanley College of Engineering and Technology for Women, Hyderabad. She is pursuing Masters in Embedded Systems from Stanley College of Engineering and Technology for Woman, Hyderabad, India.

V.Sudarshani Kataksham

received her Bachelor of Engineering degree in Electronics and communication Engineering from Jawaharlal Nehru Technological University, Hyderabad in 2009 and pursued her M.TECH in VLSI SYSTEM DESIGN from CVSR college of Engineering and Technology JNTU, Hyderabad. She is currently working as a Asst Professor in Electronics and communication Engineering Department at Stanley College of Engineering And Technology For Women ,Abids, Hyd. And she has three years of teaching experience and attended various seminars. Her areas of interest include High performance VLSI Design andVHDL based system design.

Volume No:1, Issue No:1 (June-2015)

International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

An Algorithm Based On the Iterative Computation of a Fictitious "Electrical Potential" Of the Nodes in Wireless Sensor Networks.

V.Teja
M.Tech,
Department of CST,
GITAM School of Technology, Hyderabad.

D.Vijaya Lakshmi
Assistant Professor,
Department of CST,
GITAM School of Techonology, Hyderabad.

Abstract:

A wireless sensor network can get separated into multiple connected components due to the failure of some of its nodes, which is called a "cut". In this article we consider the problem of detecting cuts by the remaining nodes of a wireless sensor network. We propose an algorithm that allows (i) every node to detect when the connectivity to a specially designated node has been lost, and (ii) one or more nodes (that are connected to the special node after the cut) to detect the occurrence of the cut. The algorithm is distributed and asynchronous: every node needs to communicate with only those nodes that are within its communication range. The algorithm is based on the iterative computation of a fictitious "electrical potential" of the nodes. The convergence rate of the underlying iterative scheme is independent of the size and structure of the network.

Keywords:
Wireless Sensor Networks, Cut in Wireless Network, Detection and Estimation, Iterative Computation.

1. Introduction:

Wireless sensor networks (WSNs) are a promising technology for monitoring large regions at high spatial and temporal resolution. However, the small size and low cost of the nodes that makes them attractive for widespread deployment also causes the disadvantage of low-operational reliability. A node may fail due to various factors such as mechanical/electrical problems, environmental degradation, battery depletion, or hostile tampering. In fact, node failure is expected to be uite common due to the typically limited energy budget of the nodes that are powered by small batteries.

Failure of a set of nodes will reduce the number of multihop paths in the network. Such failures can cause a subset of nodes—that have not failed—to become disconnected from the rest, resulting in a —cut. Two nodes are said to be disconnected if there is no path between them. We consider the problem of detecting cuts by the nodes of a wireless sensor network. May source node is a base station serves as an interface between the network and its users. So, cut may or may not separate a node from the source node, when a node is disconnected from the source is u, when a cut occurs in the network that does not separate a node u from the source node, we say that these nodes are connected, but a cut occurred somewhere (CCOS) event has occurred for u. By cut detection we mean 1) detection by each node of DOS event when it occurs, and 2) detection of CCOS events by the nodes close to a cut, and the approximate location of the cut. Nodes that detect the occurrence and approximation locations of the cuts can then alert the source node or the base station. if a node having the ability to detect the cut, it could simplywait for the network to be repaired and eventually reconnected, so it saves the energy of the multiple nodes after cut. In this paper we propose a distributed algorithm to detect cuts, named the Distributed Cut Detection (DCD) algorithm. The algorithm allows each node to detect DOS events and a subset of nodes to detect CCOS events. The algorithm we propose is distributed and asynchronous: it involves only local communication between nodes, and is robust to temporary communication failure between node pairs. A key component of the DCD algorithm is a distributed iterative computational step through which nodes compute their electrical potentials. The convergence rate of the computation is independent of the size and structure of the network.

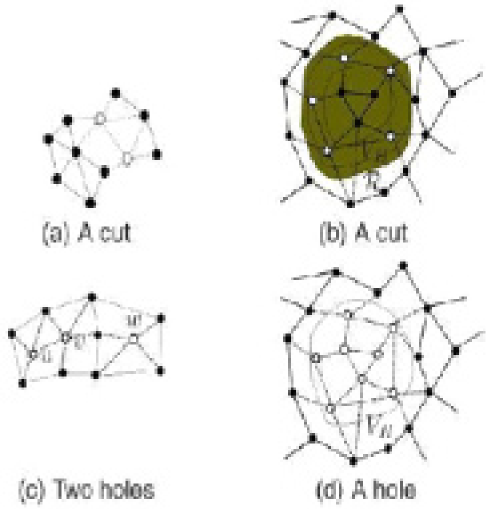


Figure 1: Examples of cut and Holes

2. EXISTING SYSTEM:

Wireless Multimedia Sensor Networks (WMSNs) hasmany challenges such as nature of wireless media and multimedia information transmission. Consequently traditional mechanisms for network layers are no longer acceptable or applicable for these networks. Wireless sensor network can get separated into multiple connected components due to the failure of some of its nodes, which is called a ―cut. Existing cut detection system deployed only for wired networks.

2.1 E-linear cut detection:

Cut detection in wireless networks has been proposed, an algorithm that can be employed by a base station to detect an e-linear cut in a network. An e- linear cut is a separation of the network across a straight line so that at least en of the nodes (n is the total number of nodes in the network) are separated from the base station. The base station detects cuts when they occur based on whether it is able to receive messages from specially placed sentinel nodes.

2.2 Flooding based scheme:

A flooding based scheme may also be used for detecting separations. Under node to- base flooding approach, every node periodically sends a time-stamped message to the base station. If the base station does not receive a new message from node i for a certain time interval, it can declare that i isdisconnected from it. Base station floods the network with time-stamped beacon packets periodically. A node detects that it is disconnected from the base if the length of time during which it hasn‘t received a new packet from the base exceeds a threshold value.

Critical node detection:

A critical node is one whose removal renders the network disconnected.

2.4 DISADVANTAGES:

Algorithm proposed only for detecting linear cuts in the networkIn flooding based technique, routes from the nodes to the base station and back have to be recomputed when node failures occur.Critical node detection uses relatively lower communication overhead come at the cost of high rate of incorrect detection.

- High false positives

- It should be emphasized that a cut can occur even if there are no critical nodes in network, when multiple non-critical nodes fail.

- Critical node detection algorithms mentioned above are designed to detect critical nodes before any node failure occurs; while the problem we address is detecting a cut after it occurs.

- Unsuitable for dynamic network reconfiguration.

- Single path routing approach

3.PROPOSED SYSTEM:

- DCD algorithm is applicable even when the network gets separated into multiple components of arbitrary shapes, and not limited to straight line cuts.

- DCD algorithm enables not just a base station to detect cuts, but also every node to detect if it is disconnected from the base station.

- CCOS event detection part of the algorithm is designed for networks deployed in 2D regions, the DOS event detection part is applicable to networks deployed in arbitrary spaces.

3.1ADVANTAGES :

•Comes with provable characterization on the DOS detection accuracy

•CCOS events detection can be identified

• DCD algorithm enables base station and also every node to detect if it is disconnected from the base station

• The DCD algorithm is distributed and asynchronous. It is robust to the temporary communication failure between the node pairs. The algorithm is iterative and has a fast convergence rate which makes it independent of size of network. Elimination of redundant information at destination nodeThe source node has the ability to detect the occurrence and location of a cut which will allow it to undertake network repair. The ability to detect cuts by both the disconnected nodes and the source node will lead to the increase in the operational lifetime of the network as a whole.

4. ASSUMPTIONS MADE:

We assume that there is a specially designated node in the network, which we call the source node. The source node may be a base station that serves as an interface between the network and its users. We can create a topology which consists of n‘ number of nodes. The number of nodes created can be done user preferences.

5. MODULE DESCRIPTION:

5.1 DISTRIBUTED CUT DETECTION:

The algorithm allows each node to detect DOS events and a subset of nodes to detect CCOS events. The algorithm we propose is distributed and asynchronous: it involves only local communication between neighboring nodes, and is robust to temporary communication failure between node pairs. A key component of the DCD algorithm is a distributed iterative computational step through which the nodes compute their (fictitious) electrical potentials. The convergence rate of the computation is independent of the size and structure of the network.

5.2 CUT:

Wireless sensor networks (WSNs) are a promising technology for monitoring large regions at high spatial and temporal resolution. In fact, node failure is expected to be quite common due to the typically limited energy budget of the nodes that are powered by small batteries.

Failure of a set of nodes will reduce the number of multi-hop paths in the network. Such failures can cause a subset of nodes – that have not failed – to become disconnected from the rest, resulting in a —cut. Two nodes are said to be disconnected if there is no path between them.

5.3 CUTS IN WIRELESS SENSOR NETWORKS:

One of the unique challenges in mobile adhoc networking environments is the phenomenon of network partitioning, which is the breakdown of a connected network topology into two or more separate, disconnected topologies.[3] Similarly sensors become fail for several reasons and the network may breaks into two or more divided partitions so can say that when a number of sensor fails so the topology changes. A node may fail due to a variety of conditions such as mechanical or electrical problems, environmental degradation, and battery reduction.

In fact, node failure is expected to be quite common anomaly due to the typically limited energy storage of the nodes that are powered by small batteries. Failure of a set of nodes will reduce the number of multichip paths in the network. Such failures can cause a subset of nodes that have not failed to become disconnected from the rest of the network, resulting in a partition of the network also called a —cut.

Two nodes are said to be disconnected if there is no path between them. And As we know that sensors has Disconnectivity from the network is normally referred as a partition of the network of cut in the wireless sensor network, which arise many problems like unreliability ,data loss, performance degradation. Because of cuts in wireless sensor network many problems may arise like a wired network means data loss problem arises, means data reach in a disconnected route.

5.4 SOURCE NODE:

We consider the problem of detecting cuts by the nodes of a wireless network. We assume that there is a specially designated node in the network, which we call the source node. The source node may be a base station that serves as an interface between the network and its users. Since a cut may or may not separate a node from the source node, we distinguish between two distinct outcomes of a cut for a particular node.

5.5 NETWORK SEPERATION:

Failure of a set of nodes will reduce the number of multi-hop paths in the network. Such failures can cause a subset of nodes – that have not failed – to become disconnected from the rest, resulting in a —cut. Because of cut, some nodes may separate from the network, that results the separated nodes can‘t receive the data from the source node.

5.6 PROBLEM DEFINITION:

When sensor wants to send data to the source node has been disconnected from the source node. Without the knowledge of the network‘s disconnected state, it may simply forward the data to the next node in the routing tree, which will do the same to its next node, and so on. However, this message passing merely wastes precious energy of the nodes; the cut prevents the data from reaching the destination.

Therefore, on one hand, if a node were able to detect the occurrence of a cut, it could simply wait for the network to be repaired and eventually reconnected, which saves on-board energy of multiple nodes and prolongs their lives. On the other hand, the ability of the source node to detect the occurrence and location of a cut will allow it to undertake network repair. Thus, the ability to detect cuts by both the disconnected nodes and the source node will lead to the increase in the operational lifetime of the network as a whole.

5.7 PROBLEM SOLUTION:

Distributed algorithm to detect cuts, named the Distributed Cut Detection (DCD) algorithm can serve as useful tools for such network repairing methods. The algorithm allows each node to detect DOS events and a subset of nodes to detect CCOS events. The algorithm proposed is distributed and asynchronous: it involves only local communication between neighboring nodes, and is robust to temporary communication failure between node pairs. A key component of the DCD algorithm is a distributed iterative computational step through which the nodes compute their (fictitious) electrical potentials. The convergence rate of the computation is independent of the size and structure of the network.

6.DISTRIBUTED CUT DETECTION ALGORITHM:

6.1 CCOS AND DOS:

When a node u is disconnected from the source, we say that a DOS (Disconnected from Source) event has occurred for u. When a cut occurs in the network that does not separate a node u from the source node, we say that CCOS (Connected, but a Cut Occurred Somewhere) event has occurred for u. By cut detection we mean (i) detection by each node of a DOS event when it occurs, and (ii) detection of CCOS events by the nodes close to a cut, and the approximate location of the cut.

A .DOS Detection:

We say that a Disconnected from Source (DOS) event has occurred for u. The algorithm allows each node to detect DOS events. The nodes use the computed potentials to detect if DOS events have occurred (i.e., if they are disconnected from the source node). The approach here is to exploit the fact that if the state is close to 0 then the node is disconnected from the source, otherwise not. In order to reduce sensitivity of the algorithm to variations in network size and structure, we use a normalized state.DOS detection part consists of steady-state detection, normalized state computation, and connection/separation detection. A node keeps track of the positive steady states seen in the past using the following method. Each node computes the normalized state difference () as follows:

xi(k) – xi(k-1) xi(k)= ------------------, if xi(k – 1)>€ zero Xi(k-1) ∞, otherwise, Where, zero is a small positive number.

A node keeps a Boolean variable Positive Steady State

Reached (PSSR) and updates PSSR(k) 1 if /( )| < for = k – Tguard , k –Tguard +1,… ,k(i.e., for Tguard consecutive iterations),where is a small positive number and Tguard is a Small integer. The initial 0 value of the state is not considered a steady state, so PSSR()=0 for =0,1, … ,Tguard.Each node keeps an estimate of the most recent —steady state observed, which is denoted by ( ). This estimate is updated at every time k according to the following rule: if PSSR( )=1, then ; otherwise – 1 . It is initialized as ss(0) = ∞.Every node i also keeps a list of steady states seen in the past, one value for each unpunctuated interval of time during which the state was detected to be steady. This information is kept in a vector ( ), which is initialized to be empty and is updated as follows: If PSSR () = 1 but PSSR(–1) = 0, then is appended to ( ) as a new entry. If steady state reached was detected in both and - 1 (i.e., PSSR( ) = PSSR(– 1) = 1, then the last entry of ( ) is updated to ( ) .

B.CCOS Detection:

When a cut occurs in the network that does not separate a node u from the source node, we say that Connected, but a Cut Occurred Somewhere (CCOS) event has occurred for u. detection of CCOS events by the nodes close to a cut, and the approximate location of the cut. By —approximate location of a cut we mean the location of one or more active nodes that lie at the boundary of the cut and that are connected to the source. To detect CCOS events, the algorithm uses the fact that the potentials of the nodes that are connected to the source node also change after the cut. However, a change in a node‘s potential is not enough to detect CCOS events, since failure of nodes that do not cause a cut also leads to changes in the potentials of their neighbors. Therefore, CCOS detection proceeds by using probe messages.

7. SYSTEM IMPLEMENTATION:

In this section, we describe the software implementation and evaluation of the DCD algorithm. In software the algorithm was implemented using the java language running on windows xp operating system.

The system executes in two phases: the Reliable Neighbor Discovery (RND) phase and the DCD Algorithm phase. In the RND phase each node is connected to the source node. Upon receiving the message, the mote updates the number of beacons received from that particular sender. To determine whether a communication link is established, each mote first computes for each of its neighbors the Packet Reception Ratio (PRR), defined as the ratio of the number of successfully received beacons and the total number of beacons sent by a neighbor. A neighbor is deemed reliable if the PRR >0:8. Next, the DCD algorithm executes. After receiving state information from neighbors, a node updates its state according to (1) in an asynchronous manner and broadcasts its new state. The state is stored in the database.

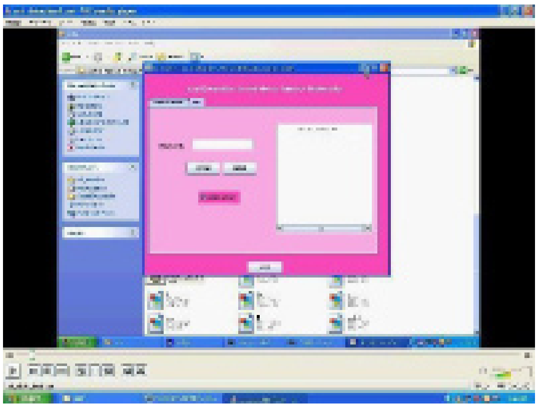


Figure 2: This screen is used for selecting file to send

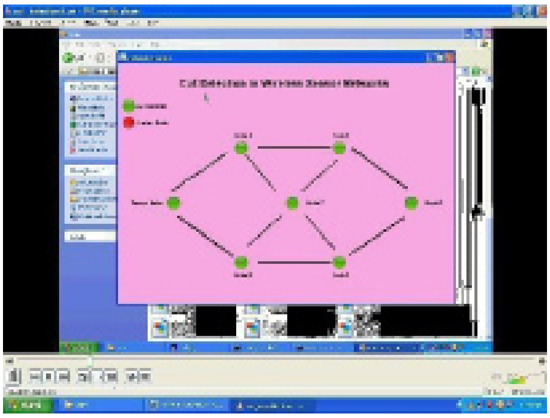


Figure 3: This screen is used for nodes representation

Volume No:1, Issue No:1 (June-2015)

International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

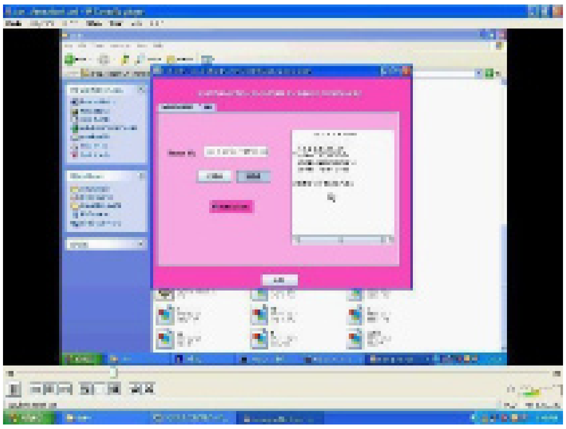


Figure 4 : This screen is used for sending file.

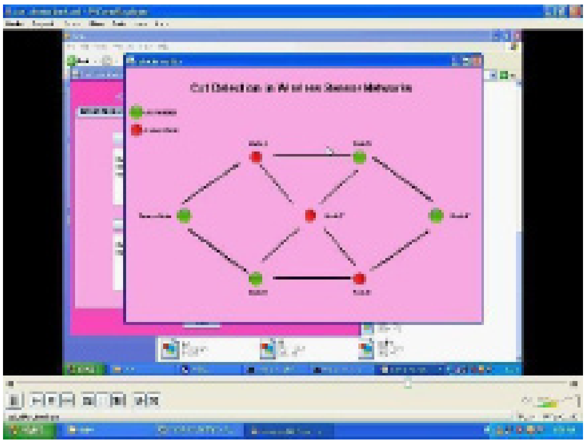


Figure 5: This screen is used for Showing Some Failure Nodes

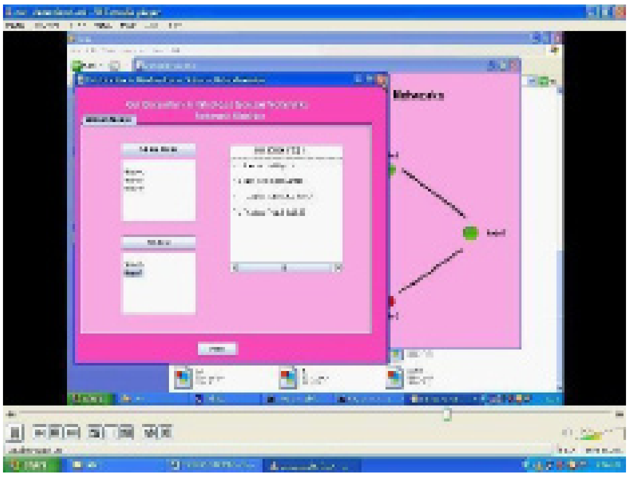


Figure 6: This screen is used for Correcting Failure Nodes

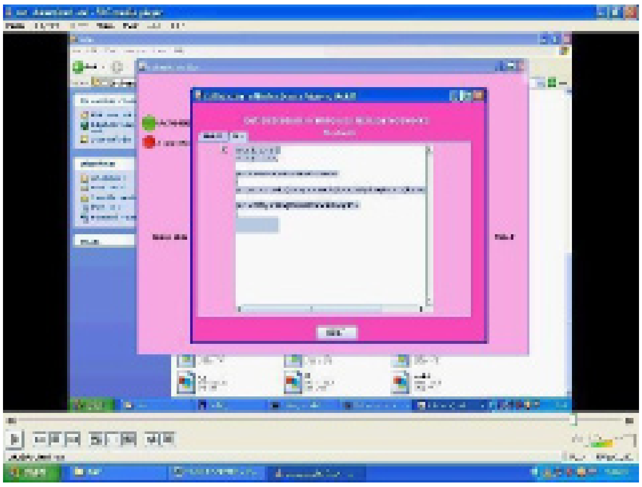


Figure 7: This screen is shows Received File

8.CONCLUSION:

The DCD algorithm we propose here enables every node of a wireless sensor network to detect DOS (Disconnected from Source) events if they occur. Second, it enables a subset of nodes that experience CCOS (Connected, but Cut Occurred Somewhere) events to detect them and estimate the approximate location of the cut in the form of a list of active nodes that lie at the boundary of the cut/hole. The DOS and CCOS events are defined with respect to a specially designated source node. The algorithm is based on ideas from electrical network theory and parallel iterative solution of linear equations. Numerical simulations, as well as experimental evaluation on a real WSN system consisting of micaz motes, show that the algorithm works effectively with a large classes of graphs of varying size and structure, without requiring changes in the parameters. For certain scenarios, the algorithm is assured to detect connection and disconnection to the source node without error. A key strength of the DCD algorithm is that the convergence rate of the underlying iterative scheme is quite fast and independent detection using this algorithm quite fast. Application of the DCD algorithm to detect node separation and reconnection to the source in mobile networks is a topic of ongoing research.

SCOPE:

A node may fail due to various factors such as mechanical/electrical problems, environmental degradation, battery depletion, or hostile tampering.

In fact, node failure is expected to be quite common due to the typically limited energy budget of the nodes that are powered by small batteries. Failure of a set of nodes will reduce the number of multi-hop paths in the network. Such failures can cause a subset of nodes that have not failed to become disconnected from the rest, resulting in a —cut. To make the network error prone, we need to identify the cut occurrence.

9.REFERENCES :

[1]G. Dini, M. Pelagatti, and I.M. Savino, "An Algorithm for Reconnecting Wireless Sensor Network Partitions," Proc. European Conf. Wireless Sensor Networks, pp. 253-267,2008.

[2]N. Shrivastava, S. Suri, and C.D. Tóth, "Detecting Cuts in Sensor Networks," ACM Trans. Sensor Networks, vol. 4, no.2,pp.1-25,2008.

[3]H. Ritter, R. Winter, and J. Schiller, "A Partition Detection System for Mobile Ad-hoc Networks," Proc. First Ann. IEEE Comm. Soc. Conf. Sensor and Ad Hoc Comm. and Networks (IEEE SECON '04), pp. 489-497, Oct.2004.

[4] M. Hauspie, J. Carle, and D. Simplot, "Partition Detection in Mobile Ad-Hoc Networks," Proc. Second Mediterranean Workshop Ad-Hoc Networks, pp. 25-27, 2003.

[5]P. Barooah, "Distributed Cut Detection in Sensor Networks," Proc. 47th IEEE Conf. Decision and Control, pp.1097-1102,Dec.2008.

[6]A.D. Wood, J.A. Stankovic, and S.H. Son, "Jam: A Jammed-Area Mapping Service for Sensor Networks," Proc.IEEE Real Time Systems Symp., 2003.

[7]J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, "System Architecture Directions for Networked Sensors," Proc. Int'l Conf. Architectural Support for Programming Languages and Operating Systems (ASPLOS), 2000.

[8]N. Shrivastava, S. Suri and C. D. T´oth. Detecting cuts in sensor networks. In Proceedings of the International Symposium on Information Processing in Sensor Networks (IPSN'05), 2005

Volume No:1, Issue No:1 (June-2015)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

Health Monitoring System Utilizing Teamviewer Software to transmit data to physicians

P. Suresh Varma
M.Tech Student,
Dept of (ECE),
Nova College of Engineering and Technology.

N. Praveen Kumar
Assistant Professor,
Dept of (ECE),
Nova College of Engineering and Technology.

Abstract:

Now a day’s healthcare industry is to provide better healthcare to people anytime and anywhere in the world in a more economic and patient friendly manner. In the present paper the physiological parameters such as ECG, Pulse rate and Temperature are obtained, processed using ARM7 LPC 2138 processor and displayed in a MATLAB graphical user interface. If any vital parameter go es out of normal range then alert SMS will be sent to Doctor Mobile. This system is utilizing Teamviewer software and low cost component to transmit ECG data to physicians for monitoring, diagnosis and patients care at a significantly low cost, regardless of patient’s location.

Index Terms:

ECG, pulse Rate, Temperature, ARM, MATLAB.

I. INTRODUCTION:

The electronics technology has entered almost in all aspects of day-to-day life, and the medical field is not exception for that. The need for well-equipped hospitals and diagnostic centers is increasing day by day as the people are becoming more conscious about their health problems. In biomedical fields special units are used, such as intensive care unit or coronary care unit.

All of these units are designed to offer the advantage of the low Nurse – Patient ratio and concentration of the equipment and the resources needed; to take care of critically ill or seriously injured units. The medical world today faces two basic problems when it comes to patient monitoring, frrstly the need of healthcare providers present bedside the patient and secondly the patient is restricted to bed and wired to large machines.

In order to achieve better quality patient care, the above cited problems have to be solved. As the technologies are advancing it has become feasible to design to horne based vital sign monitoring system to display, record and transmit signals from human body to any other location. The computer based Signal Acquisition, processing and analysis system using MATLAB to display ECG Wavefonn and filtering tool for ECG waveform. This paper discusses the aspects of acquisition of physiological Parameters like ECG Temperature, Pulse rate, pre-processing them and displaying them in a graphical user interface for being viewed by the doctor and also observe the clinically useful data, Firstly on Doctors computer and secondly on Android Mobile which contains a Teamviewer application. This system is expected to monitor patient under critical care more conveniently and accurately for diagnosing which can be interfaced with computer to bring it under a network system widely for the doctor to monitor the patient’s condition sitting in his own office without being physically present near to the patient’s bed. In second section describes system representation, third section describes Hardware description of system, fourth section describes implementation of system algorithm using arm7 LPC2138,fifth section describes simulation of ECG waveform, sixth section describes result and last section describes future scope and conclusion.

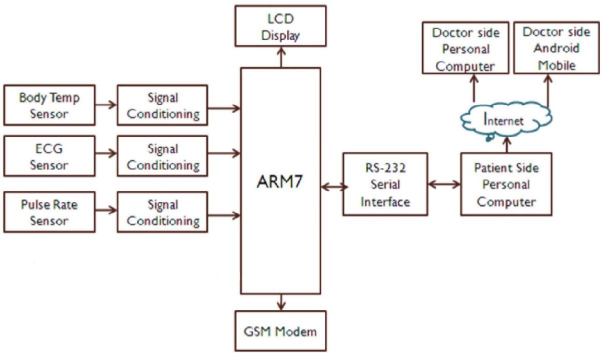


Fig. I Block Diagram of System

Volume No:1, Issue No:1 (June-2015)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

11. SYSTEM REPRESENTATION:

The block diagram of system shown in fig.1. The system contains hardware and software components. The body parameters are processed by ARM processor, it will display to the patient on LCD and Waveforms on Patient side Personal Computer using MATLAB.

The same data on computer it can be viewed by physician in two ways. Firstly on Personal Computer using Remote Desktop sharing and secondly on Android mobile having application of Remote desktop sharing. If any parameter goes abnormal then the system will sent an alert SMS to the doctor through GSM modem.

Reports indicating that system have been a great concern for physicians with a passion for technology, and barriers still remain for a low cost, comprehensive and integrated use in the daily operations.

This system reduces costs by enabling in-horne monitoring of patients, eliminating the need for utilization of expensive facilities, and reducing the need for transportation of patients to physicians and medical centers. The system is user friendlyand does not require any particular training aside from knowledge of widespread and standard Internet tools. Due to the interactive approach of the system, the physician is also able to make online consultation directly from the software provided on personal computer.

III. HARDWARE DESIGN OF SYSTEM:

The hardware design includes designing of, Temperature, Pulse rate and ECG measurement. A. Temperature Measurement The temperature sensing is performed by using a IC LM35. The LM35 se ries are precision integrated-circuit temperature sensors, whose output voltage is linearly proportional to the Celsius (Centigrade) temperature.

The output from the LM35 is given to the analog to digital converter through LM385.Analog to digital converter is inbuilt part of LPC 2138.general equation used to convert output voltage to temperature is given below

$$T(°\mathrm{C}) = Vout \ \times (\frac{100°\mathrm{C}}{Vcc})$$

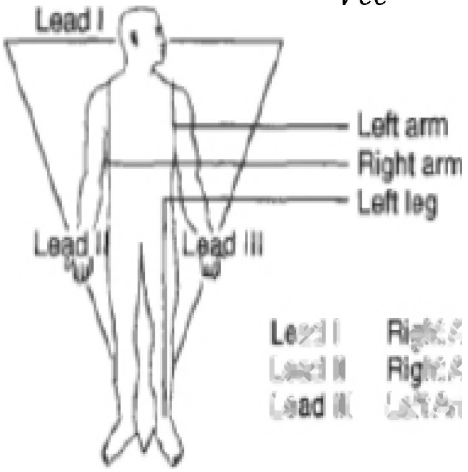


Fig. 2 Lead Placement.

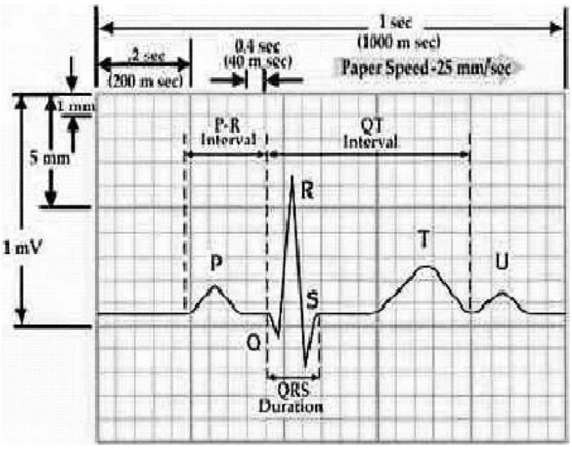
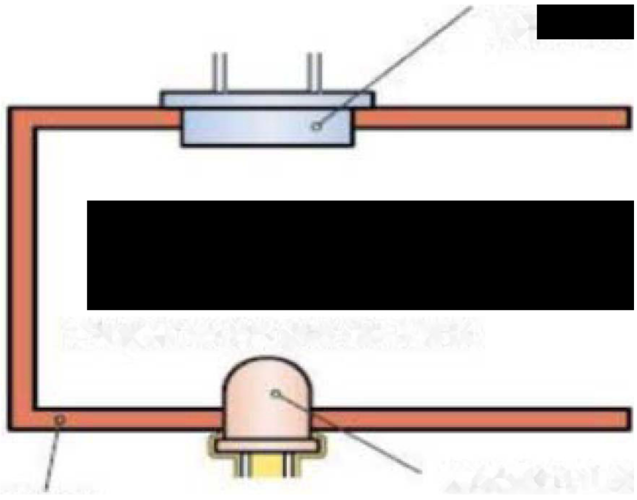


Fig. 3 ECG waveform showing QRS interval.



[redacted]

[redacted]

Fig. 4 Sensor Construction

B. Pulse rate measurement:

The sensor shown in fig. 4 consists of a super bright red LED and light detector. The LED needs to be super bright s the light must pass through finger and detected at other end. Now, when the heart pumps a pulse of blood through the blood vessels, the finger becomes slightly more opaque and so less light reached the detector. With each heart pulse the detector signal varies. This variation is converted to electrical pulse. This signal is amplified and triggered through an amplifier which outputs +5V logic level signal. The output signal is also indicated on top by a LED which blinks on each heart beat.

C. ECG measurement:

Electrodes are placed on human body as shown in fig.2.to capture small electrical voltage produced by contracting muscle due to each heartbeat. The ECG signal obtained by the electrodes is in the range of 1 to 5mV. Due to the weak voltage level, the signal is fed into an instrumentation amplifier to amplify and filter the acquired signal. The fig. 5 shows circuit diagram of ECG measurement. The amplified signal is then fed into the ARM7 LPC 2138 having inbuilt AID converter. Digital output of the ADC is sent to local terminal (patient's terminal) via an RS232 interface circuit. The parameters are the magnitude & the duration of each wave, and the intervals, such as R-R PP, Q-T and S-T intervals as shown in fig.3

a) Protection Circuit:

Diode (Dl, D2, D3, D4) are used to protect IC from over voltage when input voltage reaches to 0.7V then Diode get clamped and over voltage condition is avoided. Because of this input to instrumentation Amplifier will always be less than 0.7V.

b) Instrumentation Amplifier:

The instrumentation amplifier used is AD620 which has a very high CMRR (90dB) and high gain (1000). The AD620 is a low cost, high accuracy amplifier which requires only one extern al resistor to set gain of the amplifier.

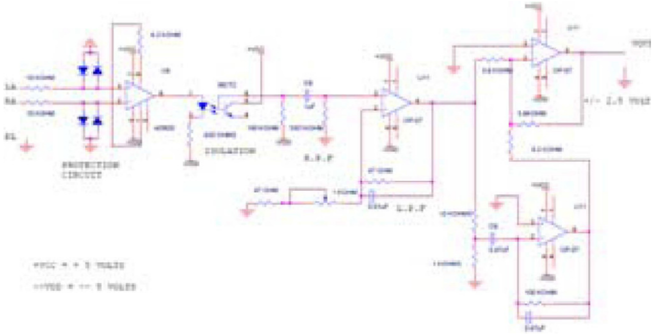


Fig. 5 Circuit Diagram of ECG Measurement

c) Isolation Circuit (IC: MCT2E):

It is NPN silicon planar phototransistor optically coupled to a gallium arsenide infrared emitting diode. Isolation circuit is used to provide isolation between input and output. It protect patient from shock. For checking the ECG signals on CRO we measure the ECG signals via CRO probes In most of the cases the Patient electrode ground and CRO ground is not the same, for such cases if the CRO ground is not properly earthed then the patient may get a Shock so for this reason we are interfacing a Opto- isolator which provides a optical insulation between the Electrode circuit and the Output circuit.

d) Bandpass Filter (0.5 Hz - 35Hz):

We take the band pass filter the frequency range of 0.5 Hz to 35 Hz. Hence we have cascaded high pass filter and low pass filter. Therefore lower cut-off frequency for HPF is 0.5 Hz.

$$fc = \frac{1}{2\pi RC} \qquad (2)$$

Where C = 1uF, R = 330kohm

Low pass filter allow signal below 35Hz only.

$$fc = \frac{1}{2\pi RC} \qquad (3)$$

Where C = 0.1uF, R = 47kohm

e) Amplijier OP07:

8 pin DIP package, low input offset voltage and high open loop gain. This non- inverting amplifier is used for signal conditioning purpose, gain provided by amplifier is 143. Total gain required for ECG circuit is 1000.Using variable resister gain adjust to 143.

j) Notch Filter:

Notch filter is used to provide zero output at particular freq. It eliminates power line noise at 50Hz. It contains H.P.F and L.P.F called twin-T network. Signal having freq between 47HZ to 53HZ .Output of notch filter is+2.5V.Output of notch filter is ±2.5V. It connects to input of adder circuit. Adder circuit shifts the signal from ±2.5V to 0-5V. And this output gives to ADC of ARM7 LPC 2138.

IV. SOFTWARE IMPLEMENT A nON OF SYSTEM USING ARM7 LPC2138:

A. Algorithm:

To implement the system using microcontroller the flow of the program i.e. algorithm which we are going to implement is as follows :

1. Initialize the microcontroller ARM7.
2. Select the input parameter.
3. Generate the start of conversion (SOC) signal for ADC through the microcontroller.
4. Wait for end of conversion (EOC) signal from the ADC.
5. Read the equivalent digital data of the parameter selected.
6. Display the received data.
7. Send the received data.
8. Select the next parameter.
9. Repeat the process.

V. SIMULATION OF ECG WAVEFORM:

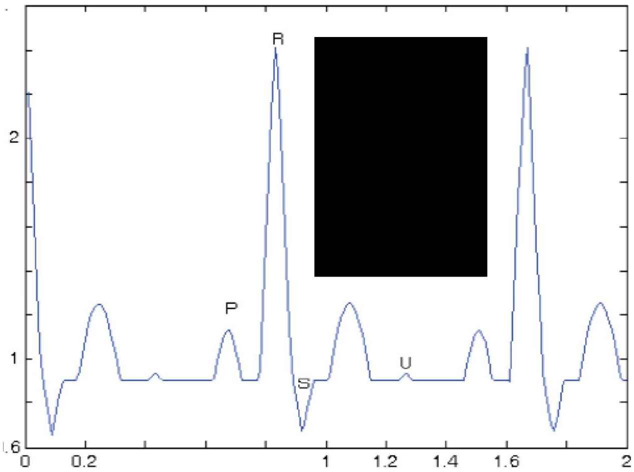
A. Using MATLAB Simulator:

The ECG Simulator is MATLAB based simulator and is able to produce Lead 11 ECG Waveform. The ECG simulator technique is used for saving time and removes difficulty of taking real time signal. We can simulate any ECG waveform using ECG simulator. ECG Signal is periodic with fundamental frequency determined by heartbeat. Fourier series can be used to representing ECG signal. The fig.3 shows single period of an ECG signal is a mixture of triangular and sinusoidal wave forms. Each significant feature of ECG signal can be represented by shifted and scaled vers ions one of these waveforms as shown below.

1. QRS, Q and S portions of ECG signal can be represented
by triangular waveforms.

2.P, T and U portions can be represented by triangular waveforms.

The generated output Signal by MA TLAB is shown in fig 6. The specifications are default for this signal which can be changed according to the user's requirement while simulating the MATLAB code. We take heartbeat as n, amplitude of P, R, Q, T waves as 25mV, 1.6mV, 0.025mV, 0.35mV respectively while the duration of P-R interval, S-T interval, P interval, QRS interval as 0.16s, 0.18s, 0.09s, 0.11srespectively.



[redacted]

Fig. 6 ECG Waveform simulated by MATLAB

VI. RESULT:

Figure 7 shows Detected ECG Signal on DSO after amplification and filtration. For instance, a display format on computer for ECG measurement is shown in Figure 8. The MA TLAB GUI program includes name of patient, Patient Report, frequency domain window displays, also display heart rate in beats per minute. The ECG waveform can be sent further through internet for further analysis. This can bring a great change in telemedicine field. ECG Waveforms can be seen by using the MATLAB Software.

A. Real time monitoring on Remote side physician Personal Computer:

The waveform on remote side physician computer is observed by using Team viewer application present on computer so doctor can take access of patient side computer desktop sharing and reports can be generated in computer also any one of the vital parameter goes abnormal then alert message will be sent to the doctor.

B. Real time monitoring on Remote side physician mobile using android application:

The waveform on remote side physician mobile is observed by using Team viewer application present on mobile so doctor can observe waveform on mobile irrespective of doctor is outside of clinic.

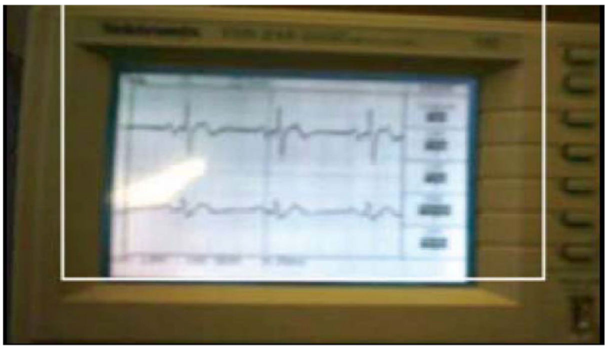


Fig. 7 Detected ECG Signal after amplification and filtration.

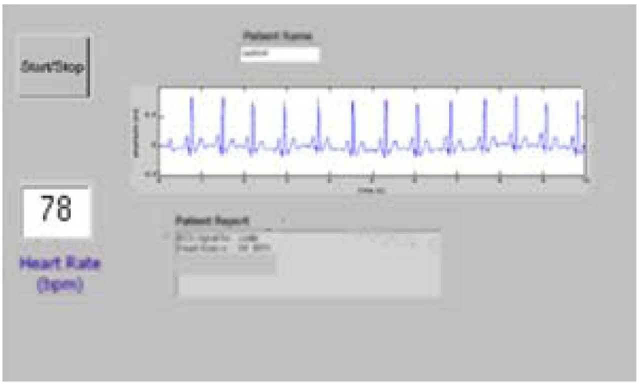


Fig. 8 MATLAB Graphics User Interface (GUI) for ECG measurement and analysis

VII. FUTURE SCOPE:

In future work the telemonitoring application is presented which allows doctor to view his patient's vital parameter remotely and dynamically in a Web page in real time and does not need to have any special requirement on his PC; all he needs is an internet access. For the patient side, it is a horne based Lab VIEW application embedded in a horne PC, during signal acquisition. The alert file is generated in Lab VIEW it will automatically send mail using Email notification application.

VIII. CONCLUSIONS:

This system reduce costs by enabling in-horne monitoring of patients, eliminating the need for utilization of expensive facilities, and reducing the need for transportation of patients to physicians and medical centers.

REFERENCES:

[1] Ya-lin Miaoi", Xiang-lin Miao, Zheng-Zhong Bian , Yong-jie Zhang Xi'an Jiaotong University, Xi'an 710049, China "Design and application of Embedded System based on ARM7 LPC2104 Processor in Telemedicine" Proceedings of the 2005 IEEE

[2] Ying-Wen Bai, Chien-Yung Cheng, Chou-Lin Lu and Yung-Song Huang, "Design and Implementation of an Embedded Remote ECG Measurement System" IMTC 2005 - Instrumentation and Measurement Technology Conference Ottawa, Canada 17-19 May 2005

[3] Nivedita Daimiwal, Asmita Wakankar, Dipali Ramdasi and Mrunal Chandratreya "Microcontroller Based ECG and Blood Press ure Simulator"- J. Instrum. Soc. India 37(4) 243-248.

[4] Mohamed Fezari, Mounir Bousbia-Salah, and Mouldi Bedda "Microcontroller Based Heart Rate Monitor" The International Arab Journal oflnfonnation Technology, Vol. 5, No. 4, October 2008.

[5] M. Chaitanya Suman, K. Prathyusha"Wireless ECG System Based on ARM LPC 2103 Processor" IJECT Vol. 3, Tssue I, Jan. - March 2012, ISSN : 2230-7109 (Online) I TSSN : 2230-9543 (Print).

[6] M. B. 1. Reaz"Tele-Health ECG Monitoring System: A Low Cost Approach" Internationallslamic University Malaysia, Kuala Lumpur, Malaysia.

[7] C.S. BUffUS, R.A. Gopinath, H. Guo, (\997) fntraductian ta Wavelets and Wavelet Trans/arms. a Primer, Prentice Halllnc.

[8] R.S. Khandpur, Handbook of Biomedical instrumentation.

Volume No:1, Issue No:1 (June-2015)

International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Implementation of Industry-Standard Routing Information Protocol (RIP) in Communication Networks

B.Kumari
(Embedded Systems)
Gokaraju Rangaraju Institute of Engineering & Technology, Hyderabad.

N.Swetha
Assistant Professor,
Gokaraju Rangaraju Institute of Engineering & Technology, Hyderabad.

ABSTRACT:

The proposed project aims on implementation of industry- standard routing information protocol (RIP) in communication networks. This rip module is built on the LINUX network services module and is IETF (internet engineering task force) compliant. An extensive set of features are supported with this RIP protocol .This is basically a control-plane software module and can integrate into a range of network processor environments. RIP become associated with transmission control/internet protocol (TCP/IP).This project is aimed to develop a rip protocol (routing information protocol)for a network processor router that has been used in local area network(LAN)to connect to broad band network .RIP takes care of dynamic routing off packets from local area network(LAN) to internet. RIP protocol works on the basis of distance vector algorithm developed by bellman-ford.Distance vector algorithm mainly explains about how to count the weight of the links directly connected to it and saves the information to its table.it handles to send route information to its neighbour routers and receive the routing table of each of its neighbors.

This project is implemented in’ C’ language .It uses GCC compiler to convert ‘C ‘code into assembly code .after converting we run the code as executable in shell of LINUX system just like system call interface and look at the packets in ethereal or WIRESHARK by using hub and a personal computer.A protocol standard is often intended to allow multiple implementations to interoperate, and multiple implementation choices and many engineering details usually make a formal protocol specification difficult. Lack of formal protocol specification has two important results, as has been shown in the IETF standard development process the correctness of the protocol is not easy to be proven; the protocol may be ambiguous in some aspects, leaving rooms for implementation bugs and even for attacks. Even worse, the bugs and ambiguities are identified in an ad hoc way, and there has not been any systematic way to identify bugs and ambiguities in existing protocols. In this work, we present a formal specification for the Routing Information Protocol (RIP). In Section 2, we will give a formal specification of the minimal requirements for a RIP router in order to guarantee that RIP will converge after a network topology change. By analyzing the RIP standards, we only specify those requirements that must be satisfied, while leaving room for any implementation choices allowed. Then in Section 3, we will present another formal specification of RIP by Finite State Machine. Using FSMs, we are able to find two ambiguities in the RIP standard.

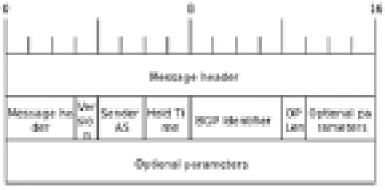
Keywords:

BGP, Split horizon, Interior gateway protocol, routing by rumor, counting to Infinity, Broadcast updates.

AIM OF THIS PROJECT:

Routing protocols use several timers that determine such variables as the frequency of routing updates, the length of time before a route becomes invalid, and other parameters. You can adjust these timers to tune routing protocol performance to better suit your internetwork needs. You can make the following timer adjustments:• The rate (time in seconds between updates) at which routing updates are sent• The interval of time (in seconds) after which a route is declared invalid• The interval (in seconds) during which routing information regarding better paths is suppressed .The amount of time (in seconds) that must pass before a route is removed from the routing table .The amount of time for which routing updates will be postponed It also is possible to tune the IP routing support in the software to enable faster convergence of the various IP routing algorithms, and, hence, quicker fallback to redundant routers.

The total effect is to minimize disruptions to end users of the network in situations where quick recovery is essential. In addition, an address family can have explicitly specified timers that apply to that address-family (or VRF) only. The timers' basic command must be specified for an address family or the system defaults for the timer's basic command are used regardless of what is configured for RIP routing. The VRF does not inherit the timer values from the base RIP configuration. The VRF will always use the system default timers unless explicitly changed using the timer's basic command.



igure1: Parameters for message format

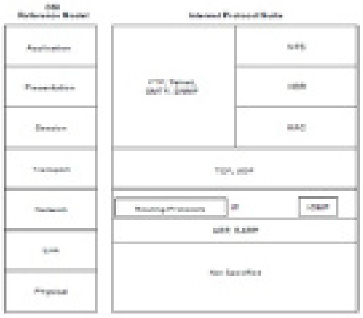


Figure2: IP packet format

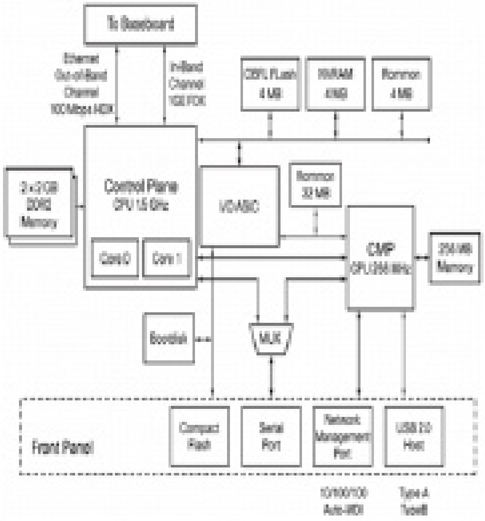


Figure 3: Message format for routing protocol

Explanation of algorithm:

Autonomous systems: The definition of an autonomous system (AS) is integral to understanding the function and scope of a routing protocol. An AS is defined as a logical portion of a larger IP network. An AS normally consists of an internetwork within an organization. It is administered by a single management authority. An AS can connect to other autonomous systems managed by the same organization. Alternatively, it can connect to other public or private networks. Some routing protocols are used to determine routing paths within an AS. Others are used to interconnect a set of autonomous systems:

- Interior Gateway Protocols (IGPs): Interior Gateway Protocols allow routers to exchange information within an AS. Examples of these protocols are Open Short Path First (OSPF) and Routing Information Protocol (RIP).

- Exterior Gateway Protocols (EGPs): Exterior Gateway Protocols allow the exchange of summary information between autonomous systems. An example of this type of routing protocol is Border Gateway Protocol (BGP).

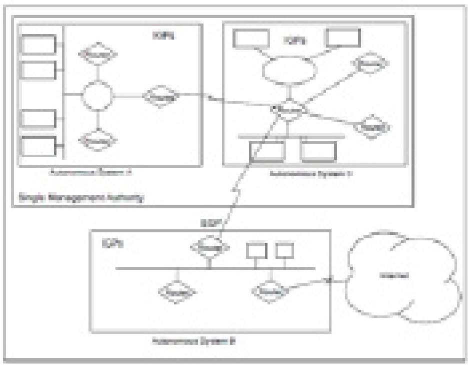


Figure 4: Types of IP routing and IP routing algorithms

Routing algorithms build and maintain the IP routing table on a device. There are two primary methods used to build the routing table:

- Static routing: Static routing uses pre-programmed definitions representing paths through the network.

- Dynamic routing: Dynamic routing algorithms allow routers to automatically discover and maintain awareness of the paths through the network.

This automatic discovery can use a number of currently available dynamic routing protocols. The difference between these protocols is the way they discover and calculate new routes to destination networks. They can be classified into four broad categories:

- Distance vector

In DV algorithms, each router has to follow these steps:

1.It counts the weight of the links directly connected to it and saves the information to its table.

2.In a specific period of time, it send its table to its neighbour routers (not to all routers) and receive the routing table of each of its neighbor's.

3.Based on the information in its neighbor's routing tables, it updates its own.

CONCLUSION:

The protocol depends upon counting to infinity to resolve certain unusual situations. As described earlier (Vector-Distance), the resolution of a loop would require either much time (if the frequency of updates was limited) or much bandwidth (if updates were sent whenever changes were detected). As the size of the routing domain grows, the instability of the vector-distance algorithm in the face of changing topology becomes apparent. RIP specifies mechanisms to minimize the problems with counting to infinity (these are described below) which allows RIP to be used for larger routing domains, but eventually RIP will be unable to cope. There is no fixed upper limit, but the practical maximum depends upon the frequency of changes to the topology, the details of the network topology itself, and what is deemed as an acceptable maximum time for the routing topology to stabilize.

FUTURE SCOPE:
RIP VERSION 2

Due to the deficiencies of the original RIP specification, RIP version 2 (RIPv2) was developed in 1993 and last standardized in 1998. It included the ability to carry subnet information, thus supporting Classless Inter-Domain Routing (CIDR).

To maintain backward compatibility, the hop count limit of 15 remained. RIPv2 has facilities to fully interoperate with the earlier specification if all Must Be Zero protocol fields in the RIPv1 messages are properly specified. In addition, a compatibility switch feature allows fine-grained interoperability adjustment .In an effort to avoid unnecessary load on hosts that do not participate in routing, RIPv2 multicasts the entire routing table to all adjacent routers at the address 224.0.0.9, as opposed to RIPv1 which uses broadcast. Unicast addressing is still allowed for special applications (MD5) authentication for RIP introduced in 1997. RIPv2 is Internet Standard STD56 (which is RFC 2453 .Route tags were also added in RIP version 2. This functionality allows for routes to be distinguished from internal routes to external redistributed routes from EGP protocols.

RIPNG: RIPng (RIP next generation), defined in RFC 2080, is an extension of RIPv2 for support of IPv6, the next generation Internet Protocol. The main differences between RIPv2 and RIPng are Support of IPv6 networking While RIPv2 supports RIPv1 updates authentication, RIPng does not. IPv6 routers were, at the time, supposed to use IPsec for authentication.RIPv2 allows attaching arbitrary tags to routes, RIPng does not RIP v2 encodes the next-hop into each route entries, RIPng specific encoding of the next hop for a set of route RIPng sends updates on UDP port 521 using the multicast group FF02::9.

REFERENCES:

[1] Bellman, R. E., "Dynamic Programming", Princeton University Press, Princeton, N.J., 1957.

[2] Bertsimas, D. P., and Gallaher, R. G., "Data Networks", Prentice-Hall, Englewood Cliffs, N.J., 1987.

[3] Braden, R., and Pastel, J., "Requirements for Internet Gateways", USC/Information Sciences Institute, RFC-1009, June 1987.

[4] Boggs, D. R., Shock, J. F., Taft, E. A., and Metcalfe, R. "Pup: An Internetwork Architecture", IEEE Transactions on Communications, April 1980.

[5] Clark, D. D., "Fault Isolation and Recovery," MIT-LCS, RFC-816, july1982.

[6] Ford, L. R. Jr., and Fulkerson, D. R., “Flows in Networks”, Princeton University Press, Princeton, N.J., 1962.

[7] Xerox Corp., “Internet Transport Protocols”, Xerox System Integration Standard XSIS 028112, December 1981.Hedrick

[8] Hedrick, C., “Routing Information Protocol”, STD 34, RFC 1058, Routers University, June 1988.

[9] Milken, G., and F. Baker, “RIP Version 2 MIB Extension”, RFC1389, January 1993.

[10] Baker, F., and R. Atkinson, “RIP-II MD5 Authentication”, RFC 2082, January 1997.

[11] Bellman, R. E., “Dynamic Programming”, Princeton University Press, Princeton, N.J., 1957.

[12] Bertsekas, D. P., and Gallaher, R. G., “Data Networks “Prentice-Hall, Englewood Cliffs, N.J., 1987.

[13] Braden, R., and Postel, J., “Requirements for Internet Gateways “, STD 4, RFC 1009, June 1987

Volume No:1, Issue No:1 (June-2015)

International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Zigbee Based Remote Controlling System for Operting Modern Appliances

Y.Duryodhana
Gokaraju Rangaraju Institute of Engineering and Technology.

ABSTRACT:

Diversification of remote control mode is the inevitable trend of development of smart appliances. In this paper we designed and developed a remote control system of smart appliances based on ZigBee wireless sensor network, realizing the diversification of remote control mode of smart appliances. The ZigBee technology is used to form a control network of household appliances within the house, two remote control networks of Internet and SMS are set up with the network interface module and GSM module. Status of the home appliances can be queried and controlled through either the remote PC interface or mobile phones. The experimental results show that: the system is reliable and can realize the remote control and inquiry of household appliances. The system has the advantages of convenient in control, flexible in adding new devices.

1. INTRODUCTION:

The advancement of remote control made development of smart appliances. The main object of this project is to provide a wireless communication link of home appliances to the remote user. This project is about controlling home appliances through wireless networks, there are two different approaches which controls the smart appliances, one through GSM network and other through Internet.

The complete project is divided into three sections Application section, Information processing section and controlling/monitoring section. Traditional way of closed system is also included by providing key at zigbee nodes. The operational parameters from application section is shared by zigbee to information processing section where these parameters are continually compared and the changed parameter values are transferred to the remote location from where we can control these smart appliances.

With the development of science and technology, Modern home environment is paid more and more attention. The number of functions has been growing; nevertheless smart appliances have formed “isolated islands” of the information, which become the bottleneck in the development of smart appliances. In addition operation near the appliances is required in traditional control mode, which limits the scope of activities. sums up the development status and analyses exiting problems of remote control system of smart appliances and then puts forward that the future trends of system will be reflected in the following three aspects: Networking technology from wired to wireless, diversification of remote control mode, energy-saving and smart will lead the new trend.Therefore, diversification of remote control mode is the inevitable trend of development of smart appliances. It’s an important part of smart home. Remote control system of smart appliances mainly consists of two parts: household internal control network and remote control network. Traditional household internal control network is generally implemented through wiring. This method is not only troublesome but also has poor scalability. Wireless network technology becomes new trends with its simple and convenient networking. ZigBee technology characterizes good security, high reliability.We have developed a remote control system of smart appliances based on wireless sensor network, applying the rapid developing mobile network and Internet to the field of remote control. The system uses a high-performing, low-costing, low-consuming chip LPC2148 as information processing center, without the high-costing PC as a local server. ZigBee technology is adopted to form household internal control network instead of the cumbersome wiring. This method requires no wiring, has a short installation period and is convenient to move and add network node. Traditional key an infrared control is included but reformed to make a diverse and various control modes. Each remotecontrol mode has account login and information matching settings to add to security of the system.

2. SYSTEM ARCHITECTURAL DESCRIPTION ARM7 FAMILY:

The ARM7 family includes the ARM7TDMI, ARM7TDMI-S, ARM720T, and ARM7EJ-S processors. The ARM7TDMI core is the industry's most widely used 32-bit embedded RISC microprocessor solution. Optimized for cost and power-sensitive applications, the ARM7TDMI solution provides the low power consumption, small size, and high performance needed in portable, embedded applications. The ARM7TDMI-S core is the synthesizable version of the ARM7TDMI core, available in both VERILOG and VHDL, ready for compilation into processes supported by in-house or commercially available synthesis libraries.

Optimized for flexibility and featuring an identical feature set to the hard macro cell, it improves time-to-market by reducing development time while allowing for increased design flexibility, and enabling >>98% fault coverage. The ARM720T hard macro cell contains the ARM7TDMI core, 8kb unified cache, and a Memory Management Unit (MMU) that allows the use of protected execution spaces and virtual memory.

This macro cell is compatible with leading operating systems including Windows CE, Linux, palm OS, and SYMBIAN OS. The ARM7EJ-S processor is a synthesizable core that provides all the benefits of the ARM7TDMI – low power consumption, small size, and the thumb instruction set – while also incorporating ARM's latest DSP extensions and Jazelle technology, enabling acceleration of java-based applications.

Compatible with the ARM9™, ARM9E™, and ARM10™ families, and Strong-Arm® architecture software written for the ARM7TDMI processor is 100% binary-compatible with other members of the ARM7 family and forwards-compatible with the ARM9, ARM9E, and ARM10 families, as well as products in Intel's Strong ARM and xscale architectures. This gives designers a choice of software-compatible processors with strong price-performance points. Figure shows the ARM7TDMI Core Diagram.The ARM7TDMI core is based on the Non Neumann architecture with a 32-bit data bus that carries both instructions and data. Load, store, and swap instructions can access data from memory. Data can be 8-bit, 16-bit, and 32-bit.

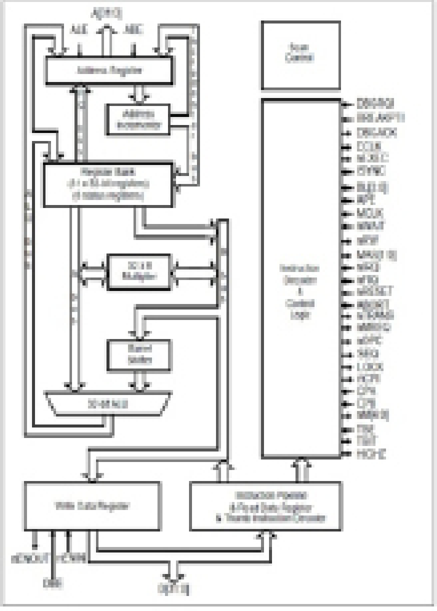


Fig: ARM7 TDMI Core Diagram

The ARM7TDMI core uses a three-stage pipeline to increase the flow of instructions to the processor. This allows multiple simultaneous operations to take place and continuous operation of the processing and memory systems.

The ARM7TDMI memory interface is designed to allow optimum performance potential and minimize memory usage. Speed critical control signals are pipelined to allow system control functions to exploit the fast-burst access modes supported by many memory technologies.

Processor states:

The ARM7TDMI processor can be in one of two states:

- ARM state
- THUMB STATE

In ARM state, 16 general registers and one or two status registers are accessible at any one time. The ARM state register set contains 16 directly accessible registers: R0 to R15. All of these except R15 are general-purpose, and may be used to hold either data or address values.

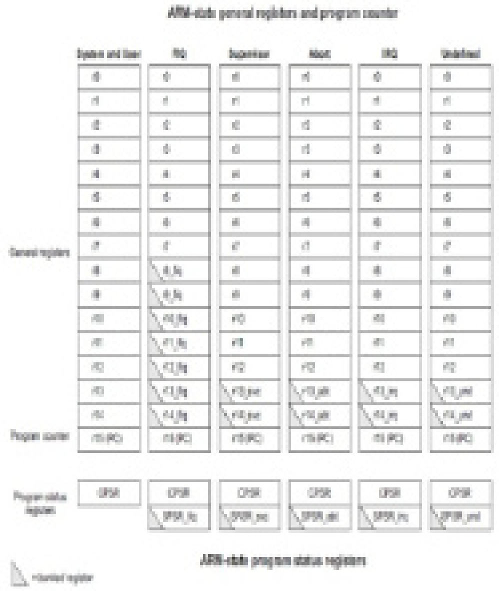


Fig: Register Organization in ARM state THUMB state

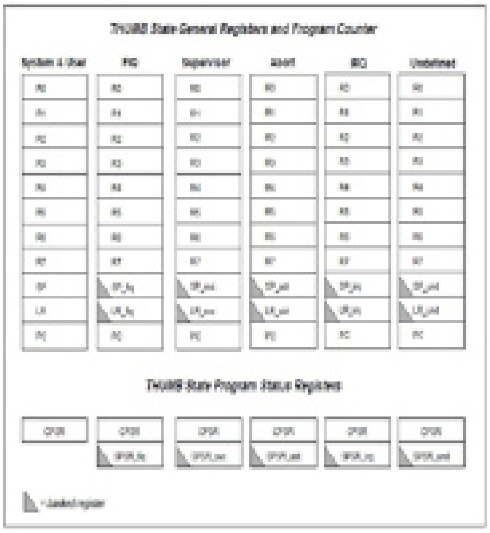

THUMB State General Registers and Program Counter
System & User
FIQ
Supervisor
Abort
IRQ
Undefined
THUMB State Program Status Registers
CPSR
= banked register

Fig: Register Organization in THUMB state

SYSTEM ISSUES AND THIRD PARTY SUPPORT:

This section contains:

- JTAG debug

- AMBA bus architecture

1. JTAG debug :

The internal state of the ARM7TDMI is examined through a JTAG-style serial interface. This allows instructions to be serially inserted into the pipeline of the core without using the external data bus. For example, when in debug state, a Store-Multiple (STM) instruction can be inserted into the pipeline. This exports the contents of the ARM7TDMI registers. This data can be serially shifted out without affecting the rest of the system.

2. AMBA bus architecture:

The ARM7 Thumb family processors are designed for use with the Advanced Microcontroller Bus Architecture (AMBA) multi-master on-chip bus architecture. AMBA is an open standard that describes a strategy for the interconnection and management of functional blocks that makes up a System-on-Chip (SoC).
The AMBA specification defines three buses:

- Advanced System Bus (ASB)

- Advanced High-performance Bus (AHB)

- Advanced Peripheral Bus (APB).

ASB and AHB are used to connect high-performance system modules. APB offers a simpler interface for low-performance peripherals. Using the ARMv7 architecture, ARM can strengthen its position as a low-power/performance leader while conquering new markets to carry its cores up in high performance and down in the low-cost high-volume domain of the microcontroller ARM designs the technology that lies at the heart of advanced digital products, from wireless, networking and consumer entertainment solutions to imaging, automotive, security and storage devices.

ARM's comprehensive product offering includes 16/32-bit RISC microprocessors, data engines, 3D processors, digital libraries, embedded memories, peripherals, software and development tools, as well as analog functions and high-speed connectivity products.

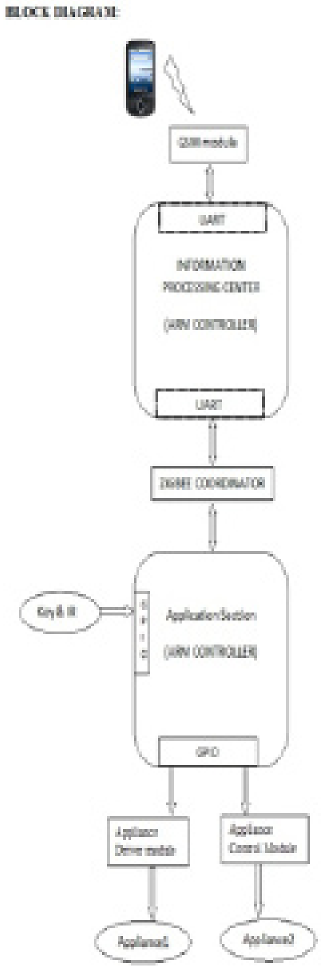


Fig: Project Design

3. MODULES DESCRIPTION:

a) LPC2148 Microcontroller:

LPC2148 microcontroller board based on a 16-bit/32-bit ARM7TDMI-S CPU with real-time emulation and embedded trace support, that combine microcontrollers with embedded high-speed flash memory ranging from 32 kB to 512 kB.

A 128-bit wide memory interface and unique accelerator architecture enable 32-bit code execution at the maximum clock rate. For critical code size applications, the alternative 16-bit Thumb mode reduces code by more than 30% with minimal performance penalty. The meaning of LPC is Low Power Low Cost microcontroller. This is 32 bit microcontroller manufactured by Philips semiconductors (NXP).

FEATURES:

- 16bit/32bit ARM7TDMI-S microcontroller in a tiny LQFP64 package.

- 40kB of on-chip static RAM and 512kB of on chip flash memory.

- In System programming/In application programming via on chip boot loader software.

- USB 2.0 full speed compliant device controller with 2kB of endpoint RAMS.

- In addition, the LPC2148 provides 8kB of on chip RAM accessible to USB by DMA.

- Two 10-bit ADCs provide a total of 14 analog inputs, with conversion times as low as 2.44 ms per channel.

- Single 10-bit DAC provides variable analog output.

- Two 32-bit timers/external event counters (with four capture and four compare channels each), PWM unit (six outputs) and watchdog.

- Low power Real-Time Clock (RTC) with independent power and 32 kHz clock input.

- Up to 45 of 5 V tolerant fast general purpose I/O pins in a tiny LQFP64 package.

- Up to 21 external interrupt pins available.

- 60 MHz maximum CPU clock available from programmable on-chip PLL with settling time of 100 ms.

- On-chip integrated oscillator operates with an external crystal from 1 MHz to 25 MHz and Power saving modes includes Idle and Power-down.

- Individual enable/disable of peripheral functions as well as peripheral clock scaling for additional power optimization.

- Processor wake-up from Power-down mode via external interrupt or BOD.

- CPU operating voltage range of 3.0 V to 3.6 V (3.3 V ± 10 %) with 5 V tolerant I/O.

b) ZIGBEE:

The XBee/XBee-PRO RF Modules are designed to operate within the ZigBee protocol and support the unique needs of low-cost, low-power wireless sensor networks. The modules require minimal power and provide reliable delivery of data between remote devices. The modules operate within the ISM 2.4 GHz frequency band and are compatible with the following:

- XBee RS-232 Adapter
- XBee RS-232 PH (Power Harvester) Adapter
- XBee RS-485 Adapter
- XBee Analog I/O Adapter
- XBee Digital I/O Adapter
- XBee Sensor Adapter
- XBee USB Adapter
- XStick
- Connect Port X Gateways
- XBee Wall Router.

The XBee/XBee-PRO ZB firmware release can be installed on XBee modules. This firmware is compatible with the ZigBee 2007 specification, while the ZNet 2.5 firmware is based on Ember's proprietary "designed for ZigBee" mesh stack (EmberZNet 2.5). ZB and ZNet 2.5 firmware are similar in nature, but not over-the-air compatible. Devices running ZNet 2.5 firmware cannot talk to devices running the ZB firmware.

The XBee modules were designed to mount into a receptacle (socket) and therefore do not require any soldering when mounting it to a board. The XBee-PRO Development Kits contain RS- 232 and USB interface boards which use two 20-pin receptacles to receive modules.

Key Features:

- High Performance, Low Cost
- Advanced Networking & Security
- Low Power
- Easy-to-Use

c) UART Data Flow:

Devices that have a UART interface can connect directly to the pins of the RF module as shown in the figure below.

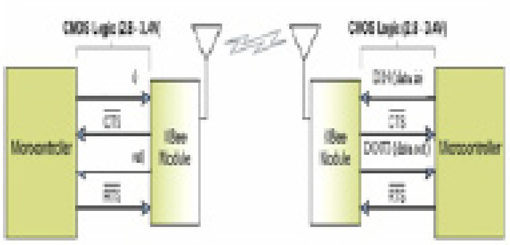


Figure 1: Zigbee UART Dataflow

Data enters the module UART through the DIN (pin 3) as an asynchronous serial signal. The signal should idle high when no data is being transmitted. Each data byte consists of a start bit (low), 8 data bits (least significant bit first) and a stop bit (high). The following figure illustrates the serial bit pattern of data passing through the module.

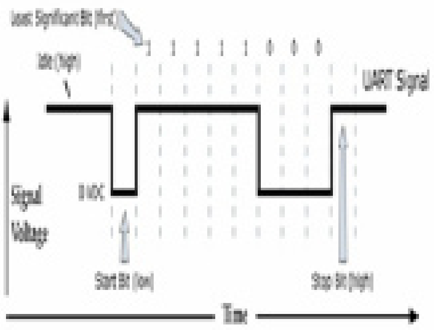


Fig: Serial Data Format

The module UART performs tasks, such as timing and parity checking, that are needed for data communications. Serial communications depend on the two UARTs to be configured with compatible settings (baud rate, parity, start bits, stop bits, data bits).

d) GSM:

Global system for mobile communication (GSM) is a globally accepted standard for digital cellular communication. GSM is the name of a standardization group established in 1982 to create a common European mobile telephone standard that would formulate specifications for a pan-European mobile cellular radio system operating at 900 MHz's GSM provides recommendations, not requirements. The GSM specifications define the functions and interface requirements in detail but do not address the hardware. The reason for this is to limit the designers as little as possible but still to make it possible for the operators to buy equipment from different suppliers. The GSM network is divided into three major systems: the switching system (SS), the base station system (BSS), and the operation and support system (OSS). The basic GSM network elements are shown in below figure .

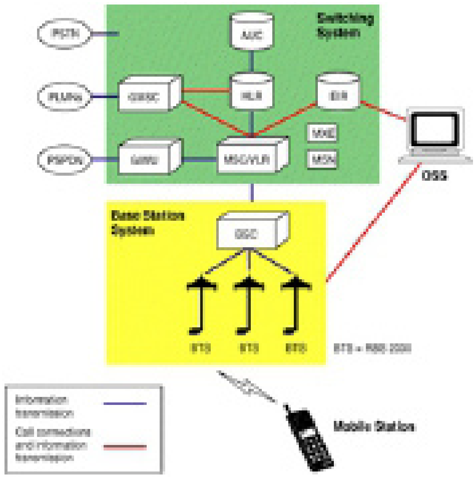


Fig: GSM Network Elements

A GSM modem is a wireless modem that works with a GSM wireless network. A wireless modem behaves like a dial-up modem. The main difference between them is that a dial-up modem sends and receives data through a fixed telephone line while a wireless modem sends and receives data through radio waves. A GSM modem can be an external device or a PC Card / PCMCIA Card. Typically, an external GSM modem is connected to a computer through a serial cable or a USB cable. A GSM modem in the form of a PC Card / PCMCIA Card is designed for use with a laptop computer. It should be inserted into one of the PC Card / PCMCIA Card slots of a laptop computer. Like a GSM mobile phone, a GSM modem requires a SIM card from a wireless carrier in order to operate.

As mentioned in earlier sections of this SMS tutorial, computers use AT commands to control modems. Both GSM modems and dial-up modems support a common set of standard AT commands. You can use a GSM modem just like a dial-up modem.

CONCLUSION:

On the basis of thorough research of ZigBee protocol, and GSM communication technology, we design and develop two types of remote control method using ARM-7 based on the high-performing, high-code-density kernel as the information processing center and adopting ZigBee module to form household internal control. We also develop a succinct functional interface in host computer.

REFERENCES:

[1] Douglas V. Hall, "Microprocessors and Interfacing Programming and Hardware", Tata McGraw-Hill Publishers, II Edition, New Delhi -1999.

[2] Kenneth J. Ayala, "The 8051 Microcontroller Architecture, Programming and Applications", Penram International, II Edition, Mumbai -1996.

[3] Mike Predko, "Programming and Customizing 8051 Microcontroller", Tata McGraw-Hill Publishers, New Delhi -1999.

[4] Muhammad Ali Mazidi, Janice Gillespie Mazidi, "The 8051 Microcontroller and Embedded systems", Pearson Education.

[5] David E Simons, "An embedded software primer".

[6] Li Wenxue, Chen Aiguo, He Lei, Gu Xiaofenng. Temperature Monitoring and Control System Based on ZigBee and GSM Technologies [J]. Micro Computer Information, 2012, 28(6): 79-81

[7] Li Kaiguo,Kang Zhiliang, Ding Wuwei, Shen Mao. Design of Appliance Control System based on TCP/IP Protocol [J]. Measurement and Control Technology, 2011,30(7): 41-45.

[8] Nan Zhongliang, Sun Guoxin. Design of Smart Home System based on ZigBee Technology [J]. Electronic Design Engineering, 2010, 18(7): 117-119.