Hardware and Software Design for Automotive Security

Nikhil Raj[1] *G. Sridhar*[2] *Dr. B. Jayachandran*[3] *M. Naresh*[4]

[1,2,3,4] *Dept of ECE, Malla Reddy College of Engineering, Secunderabad, Telangana, India*

Abstract: - Nowadays security is a major area of concern. Embedded systems are used in every automotive system. So, attack from outside network, inside networks, bugs, hacking these are common and major concerns for an automotive security. This paper aims at providing hardware and software solution for security in automotive applications. In this paper we propose a hardware model for encryption as well as a software model that can be used for security, particularly in the Automobile domain. In Automobiles 40 to 50 microcontrollers will communicate over a CAN Bus, this communication can be encrypted, it should allow only authenticate controller to communicate inside as well as outside. In vehicle there are large no of microcontrollers called ECU's which performs specific action depending on information supplied to them by other ECU's inside vehicle or the other clusters who are outside vehicle and try to communicate. This will create a wide gateway for misusing the information and manipulations. In this paper, hardware approach is presented for security build on GRP algorithm consisting of structures of Multiplexers can be called as Hardware Security Model (HSM) and in software approach by creating a gateways and only allowing authenticate controllers to communicate.

Key-Words: - ECU, Automobile, Security, Hardware, Software.

1.Introduction

Today, in vehicular networks large no of digital control units are distributed and their communication is possible over a field buses like CAN, Flex ray, MOST etc. Same information which is transmitted by one node is available with all the nodes present on the bus, proper measures should be taken to receive information correctly for the specific node. Many future applications required very high end security measures for protecting information inside automobile. This generates need for cryptographic algorithms to play an important role in security in automotive domain. Encryption like symmetric, asymmetric, encryption using digital signatures, authenticate controllers [1] these techniques will be useful to provide security from misusing or manipulating a information. In this paper above mentioned software approach is designed in Embedded C and implemented on ARM7 LPC2129 board. Similarly a software algorithm lacks rich encryption standards because of flexibility and issues like predictability. In this paper we had presented a hardware approach which is previously implemented for audio application and now can be implemented for automotive application. In this approach, a discrete structure is made by using multiplexers to do swapping with the help of control words as input to multiplexers. This control words are generated by using GRP algorithm [2] which is best suited for performing permutation and combinations. A structure is formed by using sets of multiplexers which consumes less power and can be implemented in IC form. Separate structures are created for transmitter as well as receiver. This structure provides rich encryption standards as compared to other structures [3] like EMSN, MEMS. Moreover other hardware approaches like deigning a Hardware Security Models (HSM'S) [4] is very expensive for manufacture because of inclusion of many structures like counters, algorithms though it provides top encryption standards. In this paper we are proposing a hardware model consisting of sets of 2x1 multiplexers performing permutations on GRP algorithm implemented in FPGA.

2. EVITA Model

For implementing a security application in automobiles, EVITA has proposed a hardware security model which is implemented inside automobiles. Most advanced research algorithms like AES, HASH and others are implemented to secure information. These all schemes provide rich encryption standards and it's very difficult to hack the original information. Intruder sources like an owner, service mechanic or any other person who can able to see the information and tries to corrupt

Wiki platform - An implementation for Open University

Nikhil Raj[1] Dr. Kezia Joseph[2] K. Srinivasulu[3] Dr. J. Narendra Babu[4]
[1,2,3,4] Dept of ECE, Malla Reddy College of Engineering, Secunderabad, Telangana, India

Abstract: This paper presents an ongoing implementation of a portal for students at academic specialization Automation and Applied Informatics. Through a wiki type environment - namely Doku Wiki, we implemented a collaborative site through which encourage, on the one hand, the active participation of students in solving practical laboratory activities, and on the other hand, to increase students' curiosity read educational materials before their presentation and laboratory course. In future implementations we will try to include a compiler for developing applications in C / C + +, PHP and Java. A wiki is also a natural medium for a repository for essential programming language concepts and material for teaching concepts.

Key-Words: wiki, educational site, teaching strategies

1 Introduction

What is a wiki?
A wiki is a collaborative tool that allows many people to collaborate to create and edit online documents or web pages without specialized programming skills. Many types of media formats can be incorporated in a wiki such as streams of text, images, video and RSS. The person who establishes a wiki can give other users access password protected, limiting the number of people who can edit or create content. As each edit is documented, it is possible to see a chronological list of changes made to the content, and even return back to previous versions. Many wikis also contain a number of other collaboration tools such as message boards to facilitate the process of collaboration.
Benefits of using wiki in the educational process:
- Students should not lose much time to learn how to use this technology because many features are familiar from word processors. Actually required only basic knowledge to use the wiki.
- Students can work asynchronously, i.e. not all students must be present at the same time or in the same place to provide support for team work
- Teachers can easily see that students bring their contribution in team work because each addition or modification of information is documented, making it easier for teachers evaluation.
- Similarly, the quality of student contributions can be easily monitored
- Students develop critical analysis skills and ability to constructively critique the work of their
- Many students reported that the results of group activities beyond what could be achieved individually
- The students reacted positively to the levels of support and fellowship that we have received from others Integrate students as part of the collaborative process. They also submitted that they began to know colleagues better in most cases.
- At first, many students expressed doubt about their ability to work collaboratively online and yet, at the end of activities, many were surprised and impressed by what they have achieved collectively.
Issues to be highlighted:
- Students may not know how to work effectively in groups. It is therefore necessary support and guidance from teachers
- Technical assistance should be provided to enable students to obtain skills in the effective use of wikis
- The first iteration of the class consumes significant time to develop structure, evaluating and creating technical resources support to students, but this meant that subsequent iterations spent minimal time for the introduction of information.

1.1 Types of wiki-based interaction

The term “wiki” is an acronym for “What I Know Is” [15]. In technology terms, a wiki is an editable website whereusers are able to create hyperlinks, insert images, and modify text [15] [8] [16]. The integration of wikis into lessonsand assessments is grounded in the theory of social constructivism [8]. Wikis can be an effective instructionalstrategy because they promote learning by enhancing interaction and empowering students in the educationalprocess. Three types of interaction are supported by wiki-based instruction: learner-content, learner-instructor,and learner-learner [11]. Wikis also provide additional opportunities outside the classroom setting for students tointeract with the course content, each other, and the instructor. When

Design of A Low Cost Extendable Embedded Smart Car Security System

Dr. M. N. Yadav[1] K. Srinivasulu[2] Dr. Vaibhav Meshram[3] D. Kiran[4]

[1,2,3,4] Dept of ECE, Malla Reddy College of Engineering, Secunderabad, Telangana, India

Abstract - The main aim of this proposed embedded car security system is, If the car is stolen, this system is designed to retrieve the position of the car and the car thief, and make an alarm loudly or soundlessly. The other modules transmit necessary information to users and help to keep eyes on cars all the time, even when the car is lost. Which consists of a face detection subsystem, a GPS module, a GSM module and a control platform? It captures the image using a camera which will be hidden in the dash board. Face Detection Algorithm is used to detect the face., In today's world, many new techniques such as biometric recognition technique, image processing technique, communication technique and so on, have been integrated into car security systems. At the same time, the amount of car lost is also increasing. The system is mainly used to identify the car and the thief who theft the car. This system prototype is built on the base of one embedded platform ARM7 which controls all the processes. Experimental results illuminate the validity of this car security system.

Keywords– Vehicle Security Camera; GPS; GPRS; embedded system, ARM7.

I. INTRODUCTION

This proposed embedded car security system, FDS (Face Detection System) is used to detect the face of the driver and compare it with the predefined faces. For example, in the night when the car's owner is sleeping and someone theft the car then FDS obtains images by one tiny web camera which can be hidden in the car. FDS compares the obtained image with the predefined images if the image doesn't match, then the information is sent to the owner through MMS.So now owner can obtain the image of the thief in his mobile as well as he can trace the

Location-Aware and Safer Cards

M. Shiva Kumar[1] B. H. Leena[2] Dr. K. Srinivasulu[3] K. Deepak Babu[4]
[1,2,3,4] Dept of ECE, Malla Reddy College of Engineering, Secunderabad, Telangana, India

Abstract— **In this paper, we report on a new approach for improving security and privacy in certain RFID applications whereby location or location-related information (such as speed) can serve as a legitimate access context. Examples of these applications include access cards, toll cards, credit cards, and other payment tokens. We show that location awareness can be used by both tags and back-end servers for defending against unauthorized reading and relay attacks on RFID systems. On the tag side, we design a location-aware selective unlocking mechanism using which tags can selectively respond to reader interrogations rather than doing so promiscuously. On the server side, we design a location-aware secure transaction verification scheme that allows a bank server to decide whether to approve or deny a payment transaction and detect a specific type of relay attack involving malicious readers.**

The premise of our work is a current technological advancement that can enable RFID tags with low-cost location (GPS) sensing capabilities. Unlike prior research on this subject, our defenses do not rely on auxiliary devices or require any explicit user involvement.

Keywords- Context Recognition,RFID, Mobile Payment System, Relay Attacks, Location Sensing.

I. INTRODUCTION

Low cost, small size and the ability of allowing computerized identification of objects make Radio Frequency Identification (RFID) systems increasingly ubiquitous in both public and private domains. Prominent RFID applications supply chain management (inventory control), e-passports, credit cards, driver's licenses, vehicle systems (toll collection or car key), access cards (building, parking or public transport), and medical implants. NFC, or Near Field Communication, is yet another upcoming RFID technology that allows devices, such as smart phones, to have both RFID tag and reader functionality. In particular, the use of NFC-equipped mobile devices as payment tokens (such as Google Wallet) is considered to be the next generation payment system and the latest buzz in the financial industry.

A typical RFID system consists of tags, readers, and/or back-end servers. Tags are miniaturized wireless radio devices that store information about their corresponding subject. Such information is usually sensitive and personally identifiable. For example, a US e-passport stores the name, nationality, date of birth, digital photograph, and (optionally) fingerprint of its owner. Readers broadcast queries to tags in their radio transmission ranges for information contained in tags and tags reply with such information. The queried information is then sent to the server (which may coexist with the reader) for further processing and the processing result is used to perform proper actions (such as updating inventory, opening gate, charging toll or approving payment).

Due to the inherent weaknesses of underlying wireless radio communication, RFID systems are plagued with a wide variety of security and privacy threats. A large number of these threats are due to the tag's promiscuous response to any reader requests. This renders sensitive tag information easily subject to unauthorized reading. Information (might simply be a plain identifier) gleaned from a RFID tag can be used to track the owner of the tag, or be utilized to clone the tag so that an adversary can impersonate the tag's owner.

Promiscuous responses also incite different types of relay attacks. One class of these attacks is referred to as "ghostand-leech". In this attack, an adversary, called a "leech," relays the information surreptitiously read from a legitimate RFID tag to a colluding entity known as a "ghost." The ghost can then relay the received information to a corresponding legitimate reader and vice versa in the other direction. This way a ghost and leech pair can succeed in impersonating a legitimate RFID tag without actually possessing the device.

A more severe form of relay attacks, usually against payment cards, is called "reader-and-ghost"; it involves a malicious reader and an unsuspecting owner intending to make a transaction in this attack, the malicious reader, serving the role of a leech and colluding with the ghost, can fool the owner of the card into approving a transaction which she did not intend to make (e.g., paying for a diamond purchase made by the adversary while the owner only intending to pay for food). We note that addressing this problem requires secure transaction verification, i.e., validation that the tag is indeed authorizing the intended payment amount.

The feasibility of executing relay attacks has been demonstrated on many RFID (or related) deployments, including the Chip-and-PIN credit card system, RFID assisted voting system, and keyless entry and start car key system. With the increasingly ubiquitous deployment of RFID applications, there is a pressing need for the development of security primitives and protocols to defeat unauthorized reading and relay attacks. However, providing security and privacy services for RFID systems presents a unique and formidable set of challenges. The inherent difficulty stems

Error Correction in Extended Orthogonal Latin Square Codes using Syndrome Fault Detection and Majority Logic Decoding

Dr. J. Narendra Babu[1] *Dr.P. John Paul*[2] *B.C. Nirmala*[3] *M. Chandramohan*[4]
[1,2,3,4] *Dept of ECE, Malla Reddy College of Engineering, Secunderabad, Telanagana, India*

Abstract—**Error correction codes (ECCs) are commonly used to Protect memories from errors. As multi-bit errors become more frequent, single error correction codes are not enough and more advanced ECCs are needed. The use of advanced ECCs in memories is, however, limited by their decoding complexity. In this context, one-step majority logic decodable (OS-MLD) codes are an interesting option as the decoding is simple and can be implemented with low delay. Orthogonal Latin squares (OLS) codes are OS-MLD and have been recently considered to protect caches and memories. The main advantage of OLS codes is that they provide a wide range of choices for the block size and the error correction capabilities. We can also extend these codes to accommodate more number of data bits thus reducing the overhead. But most of the time all the words in the memory are not error prone, but still we try to decode them and waste clock cycles on it. In this brief, a method is presented to detect whether an error is present in the code word and if present then only the correction is done using majority logic decoding.**

Keywords—***Error correction codes (ECCs), Extended Orthogonal Latin squares, Syndrome fault detection (SFD), majority logic decoding, and memory***.

I. INTRODUCTION

To mitigate errors, error correction codes (ECCs) are commonly used in memories [1]. Because of their simplicity, single error correction codes that can correct one bit per word are traditionally used [2]. Other codes that can also correct double adjacent errors [3] or double errors in general have also been studied [4]. Codes that can correct more errors have a larger impact on delay and power that can limit their applicability to memory designs [5]. One alternative to minimize those impacts is to use codes that are one-step majority logic decodable (OS-MLD). OS-MLD codes can be decoded with low latency and are, therefore, attractive to protect memories [6]. Several types of OS-MLD codes have been proposed for memory protection. One example is a type of Euclidean geometry (EG) codes studied in [7] and [8].

EG codes provide a limited number of block sizes and error correction capabilities. For example, for double error correction (DEC), only very small data block sizes (smaller than 16 bits) can be implemented. In addition, the error correction capability for a block size is fixed and cannot be adapted to the error rate. Another type of code that is OSMLD is orthogonal Latin squares (OLS) code [11]. OLS codes can be implemented for a wide range of block sizes and error correction capabilities. This flexibility and the simple and fast decoding are the main advantages of OLS codes. However, OLS codes typically require more parity bits than other codes to correct the same number of errors. In some applications, this disadvantage is offset by their modularity and the simple and low delay decoding implementation (as OLS codes are OS-MLD). For example, OLS codes have been recently considered to protect memories [12], caches [13], and interconnections [14].

The rest of this brief is organized as follows. Section II provides an overview of OLS and Extended OLS codes summarizing some of their properties that are used in the rest of this paper. Then, the proposed method for error detection and correction is presented in Section III. Section IV speaks of the results. Finally, the conclusions are presented in Section V.

II. OLS and Extended OLS Codes

A Latin square of size m is an $m \times m$ matrix that has permutations of the digits 0, 1, …, and $m - 1$ in both its rows and columns [15].Two Latin squares are said to be orthogonal if when they are superimposed every ordered pair of elements appears only once. OLS codes are derived from OLS [11]. The block sizes for OLS codes are $k = m2$ data bits and 2 tm parity bits, where t is the number of errors that the code can correct and m is an integer. For a given pair of values of t and m, the corresponding OLS code exists only if there are at least $2t$ OLS of size m.

The extended codes have the same number of parity bits as the original OLS codes but a larger number of data bits. Therefore, the relative overhead is smaller. The derived codes can be decoded using OS-MLD as the original OLS codes. The decoding area and delay are also similar. Therefore, the

PERSONAL HEALTH MONITORING WITH ANDROID BASED MOBILE DEVICES

Dr. K. Srinivasulu[1] Dr. J. Narendra Babu[2] Dr. Vaibhav Meshram[3] Kavitha[4]
[1,2,3,4] Dept of ECE, Malla Reddy College of Engineering, Secunderabad, Telangana, India

ABSTRACT: Patient monitoring systems are gaining their importance as the fast-growing global elderly population increases demands for caretaking. These systems use wireless technologies to transmit vital signs for medical evaluation. The aim of the project is to provide a better health care to people from house in more economic and pertinent friendly manner. The need of home based health monitoring system is increased now days because health care cost is increasing exponentially in last few decades. In the proposed home based health monitoring system using android smart phone includes the aspects of acquisition of medical parameters like Body temperature, Pulse rate and ECG. Processing of a collected data using ARM7 (LPC2148) processer and processed data is then displayed on doctors or relatives android mobile phones. Also the data can be displayed on personal computer. The system is utilizing a low cost component to transmit data like ECG to physician for monitoring; diagnosis and patients care at significantly low cost, regardless of patient's location.

KEY WORDS- **medical evaluation, android smart phone, aspects of acquisition, ECG, ARM7 (LPC2148), Diagnosis**

INTRODUCTION:

In intensive care units, there are provisions for continuously monitoring patients. Their heart rates, temperatures, ECG etc. are continuously monitored. But in many cases, patients get well and come back to home from hospital. But the disease may return, he may get infected with a new Disease, there may be a sudden attack that may cause his death. So in many cases, patients are released from hospital but still they are strongly advised to be under rest and observation for some period of time (from several days to several months). In these cases, our system can be quite handy. Patient's data (temperature, heart rate, ECG etc.) will be frequently measured and sent to server. Period of sending (say every 3 min) can be set. Heart rates can be sent every minute and temperatures can be sent after half an hour etc. But these can be parameterized to ensure that when a patient is normal, not many readings will be sent so that sensors have a longer life-time. But when the patient is ill, readings will be taken frequently and sent to server.

Monitoring person learns patient specific threshold. Say the regular body temperature of a patient is 37 c whereas one person feels feverish if his body temperature is 37.0 c. By employing an averaging technique over a relatively long time, Observer can learn these thresholds for patients. Using android application, one can view his medical history date wise, event wise etc. android application can perform data mining on a particular patient data to discover important facts. Suppose a person has medium high temperature that starts at evening and lasts till midnight. If this phenomenon continues for several days, observer can detect this fact and inform to doctors saying "You frequently have short-period fever that may be a symptom of a bad disease. Consult patient immediately". This system can transmit continuously data. Suppose a patient has come back home after cardiac surgery. If the patient has cardiac problems like arrhythmia, then there will be irregular variation of heart signal. This may occur only once or twice a day. But if system transmits continuous data, such variations will be immediately detected and alerts will be issued.

I. HARDWARE SYSTEM:

Micro controller: This section forms the control unit of the whole project. This section basically consists of a Microcontroller with its associated circuitry like Crystal with capacitors, Reset circuitry, Pull up resistors (if needed) and so on. The Microcontroller forms the heart of the project because it controls the devices being interfaced and communicates with the devices according to the program being written.

ARM7TDMI: ARM is the abbreviation of Advanced RISC Machines, it is the name of a class of processors, and is the name of a kind technology too. The RISC instruction set, and related decode mechanism are much simpler than those of Complex Instruction Set Computer (CISC) designs.

DESIGN AND IMPLEMENTATION OF BCH CODE FOR ERROR DETECTION AND CORRECTION OF DIGITAL SYSYEMS

P. Venkateshwarlu[1,] B. Manjula[2] G. Sanjeev[3] S. Krishna Kishore[4]
[1,2,3,4] Dept of ECE, Malla Reddy College of Engineering, Secunderabad, Telangana, India

Abstract— **In general Error correction codes (ECCs) are commonly used to protect memories against errors. Among ECCs, OLS codes have gained renewed interest for memory protection due to their modularity and simplicity of the decoding algorithm that enable slow delay implementations. An important issue is that when ECCs is used, the encoder and decoder circuits can also suffer errors. The proposed method uses a concurrent error detection technique for the properties of BCH codes to efficiently implement a parity prediction scheme that detects all errors that affect a single circuit node, which reduces the parity bits, area, error detection and correction delay and its performance is simulated by using Xilinx**

***Key words*- Error correction codes, OLS codes, BCH codes, correction delay**

I. INTRODUCTION

Error correction codes (ECCs) have been utilized to secure memories for a long time. There will be a wide range of codes that will be utilized or have been proposed for memory applications. Single Error Correction(SEC) codes that can amend one bit for every statement are normally utilized. More exceptional codes that can additionally right twofold contiguous lapses or twofold slips by and large have likewise been mulled over. The utilization of more mind boggling codes that can revise more mistakes will be restricted by their effect on delay and power, which can limit their materialness to memory outlines.

To defeat those issues, the utilization of codes that are one step majority logic decodable (OS-MLD) has as of late been proposed. OS-MLD codes might be decoded with low idleness and are, accordingly, used to ensure memories. Among the codes that are OS- MLD, a sort of Euclidean geometry (EG) code has been proposed to secure memories. The utilization of distinction set code has additionally been as of late dissected in. An alternate kind of code that is OS-MLD is BCH code .The utilization of BCH codes has picked up reestablished enthusiasm for interconnections, memories, and stores. This is because of their seclusion such that the lapse revision abilities might be effortlessly adjusted to the blunder rate or to the mode of operation. RS codes regularly require more equality bits than different codes to revise the same number of lapses. The rest of this brief is organized as follows. Section II provides an overview of OLS and Extended OLS codes summarizing some of their properties that are used in the rest of this paper. Then, the proposed method for error detection and correction is presented in Section III. Section IV speaks of the results. Finally, the conclusions are presented in Section V.

Notwithstanding, their measured quality and the straightforward and low defer disentangling usage (as BCH codes are OS-MLD), counterbalance this inconvenience in numerous applications. A vital issue is that the encoder and decoder circuits required to utilize (Eccs) can likewise endure lapses. At the point when a slip influences the encoder, an inaccurate word may be built into the memory.

II VARIOUS CODE TECHNIQUES:

1. DUPLEX SYSTEM:

A duplex framework is an illustration of a traditional excess plan that might be utilized for simultaneous lapse location demonstrates the fundamental structure of a duplex framework. Duplication has been utilized for simultaneous mistake location as a part of various frameworks including the Bell Switching System, from organizations like Stratus and Sequoia. In any duplex framework there are two modules (indicated in Fig. 2.1 as Module 1 and Module 2) that actualize the same rationale capacity. The two executions are not so much the same. A comparator is utilized to check whether the yields from the two modules concur. On the off chance that the yields deviate, the framework demonstrates a lapse. For a duplex framework,

Performance Analysis of Linear and Nonlinear Resource Allocation Techniques in OFDM System

M. Naresh[1] *Dr.B. Jayachandran [2]* *Dr. D. Kiran[3]* *Dr. N. Rajesha [4]*
[1,2,3,4] Dept of ECE, Malla Reddy College of Engineering, Secunderabad, India.

Abstract— **Multiuser orthogonal frequency division multiplexing(MU-OFDM) is promising technique for achieving high downlink capacities in future cellular and wireless LAN systems OFDM base stations allows multiple users transmitter simultaneously on different sub carrier during the same symbol period. The sum capacity of MU-OFDM is maximized when each sub channel is assigned to the user with best channel to noise ratio for that sub channel in this paper we focus the base station resource allocation in terms of sub carrier and power to each user to maximize the sum of user data rates subject to constraints on total power bit error rate and proportionality among user data rate there are number of methods proposed in the literature which are being iterative non linear methods which has suitable for offline optimization in the special I sub-channel SNR case and iterative route finding method has linear time complex city in the number of users and NlogN complexity in the number of sub-channels the proposed method is low complex method which works under waving the restriction of high sub channel SNR and yields higher user data rates it is also shown that with the proposed resource allocation algorithm sum capacity is distributed more fairly and flexibility among users then the sum capacity maximization method.**

Keywords- MU-OFDMA, SNR, Resource Allocation

I. INTRODUCTION

OFDMA, also referred to as Multiuser-OFDM is being considered as a modulation and multiple access method for 4th generation wireless networks OFDMA is an extension of Orthogonal Frequency Division Multiplexing (OFDM), which is currently the modulation of choice for high speed data access systems such as IEEE 802.11a/g wireless LAN and IEEE 802.16a fixed wireless broadband access systems.

Orthogonal frequency division multiplexing (OFDM) is a promising technique for the next generation of wireless communication systems.

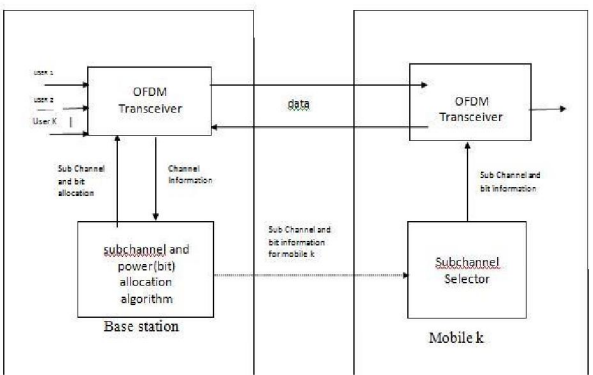
OFDM divides the available bandwidth into *N* orthogonal sub-channels. By adding a cyclic prefix (CP) to each OFDM symbol, the channel appears to be circular if the CP length is longer than the channel length. Each sub channel thus can be modeled as a time-varying gain plus additive white Gaussian noise (AWGN). Besides the improved immunity to fast fading brought by the multicarrier property of OFDM systems, multiple access is also possible because the sub channels are orthogonal to each other.

OFDM adds multiple access to OFDM by allowing a number of users to share an OFDM symbol. Two classes of resource allocation schemes exist: fixed resource allocation and dynamic resource allocation [. Fixed resource allocation schemes, such as Time Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA), assign an independent dimension, e.g. time slot or sub-channel to each user. A fixed resource allocation scheme is not optimal since the scheme is fixed regardless of the current channel condition. On the other hand, dynamic resource allocation allocates a dimension adaptively to the users based on their channel gains. Due to the time-varying nature of the wireless channel, dynamic resource allocation makes full use of multiuser diversity to achieve higher performance.

The problem of assigning subcarriers and power to the different users in an OFDMA system has recently been an area of active research. In the margin-adaptive resource allocation problem was tackled, wherein an iterative subcarrier and power allocation algorithm was proposed to minimize the total transmit power given a set of fixed user data rates and bit error rate (BER) requirements. In the rate-adaptive problem was investigated, wherein the objective was to maximize the total data rate over all users subject to power and BER constraints. It was shown in that in order to maximize the total capacity, each subcarrier should be allocated to the user with the best gain on it, and the power should be allocated using the water-lling algorithm across the subcarriers. However, no fairness among the users was considered in this problem was partially addressed by ensuring that each user would be able to transmit at a minimum rate, and also in by incorporating a notion of fairness in the resource allocation through maximizing the minimum user's data rate. In the fairness was extended to incorporate varying priorities. Instead of maximizing the minimum user's capacity, the total capacity was maximized subject to user rate proportionality constraints. This is very useful for service level differentiation, which allows for flexible billing mechanisms for different classes of users. However, the algorithm proposed in involves solving non-linear equations, which requires computationally expensive iterative operations and is thus not suitable for a cost-effective real-time implementation.

This paper extends the work in by developing a sub-carrier allocation scheme that linearizes the power allocation problem while achieving approximate rate proportionality. The resulting power allocation problem is thus reduced to a solution to simultaneous linear equations. In simulation, the proposed algorithm achieves a total capacity that is consistently higher than the previous work, requires significantly less computation, while achieving acceptable rate proportionality.

II. SYSTEM MODEL



Hybrid High Noise resiliency Pitch Detection Algorithm

Dr. M Narsing Yadav[1] *Dr. J. Narendra Babu*[2] *Dr. Kezia Joseph*[3] *Dr. Vaibhav Meshram*[4]
[1,2,3,4] *Dept of ECE, Malla Reddy College of Engineering, Secunderabad, Telangana, India*

Abstract— **Pitch is one of the essential features in many speech related applications. A pitch detection algorithm (PDA) is an algorithm designed to estimate the pitch or fundamental frequency of a quasiperiodic or virtually periodic signal, usually a digital recording of speech or a musical note or tone. This can be done in the time domain or the frequency domain or both the two domains. Although numerous pitch detection algorithms have been developed, as shown in this paper, the detection ratio in noisy environments still needs improvement. In this paper, we present a hybrid noise resilient pitch detection algorithm named BaNa that combines the approaches of harmonic ratios and Cepstrum analysis. A Viterbi algorithm with a cost function is used to identify the pitch value among several pitch candidates. We use an online speech database along with a noise database to evaluate the accuracy of the BaNa algorithm and several stateof-the-art pitch detection algorithms. Results show that for all types of noises and SNR values investigated, BaNa achieves the best pitch detection accuracy. Moreover, the BaNa algorithm is shown to achieve around 80% pitch detection ratio at 0dB signalto-noise ratio (SNR).**

Keywords- Pitch detection, noise resilience, harmonics, Viterbi algorithm

I. INTRODUCTION

A pitch detection algorithm (PDA) is an algorithm designed to estimate the pitch or fundamental frequency of a quasiperiodic or virtually periodic signal, usually a digital recording of speech or a musical note or tone. This can be done in the time domain or the frequency domain or both the two domains.

PDAs are used in various contexts (e.g. phonetics, music information retrieval, speech coding, musical performance systems) and so there may be different demands placed upon the algorithm. There is as yet no single ideal PDA, so a variety of algorithms exist, most falling broadly into the classes given below.[1]

In the time domain, a PDA typically estimates the period of a quasiperiodic signal, then inverts that value to give the frequency.

One simple approach would be to measure the distance between zero crossing points of the signal (i.e. the Zero-crossing rate). However, this does not work well with complex waveforms which are composed of multiple sine waves with differing periods. Nevertheless, there are cases in which zero-crossing can be a useful measure, e.g. in some speech applications where a single source is assumed. The algorithm's simplicity makes it "cheap" to implement.

More sophisticated approaches compare segments of the signal with other segments offset by a trial period to find a match. AMDF (average magnitude difference function), ASMDF (Average Squared Mean Difference Function), and other similar autocorrelation algorithms work this way. These algorithms can give quite accurate results for highly periodic signals. However, they have false detection problems (often "*octave errors*"), can sometimes cope badly with noisy signals (depending on the implementation), and - in their basic implementations - do not deal well with polyphonic sounds (which involve multiple musical notes of different pitches).

Current time-domain pitch detector algorithms tend to build upon the basic methods mentioned above, with additional refinements to bring the performance more in line with a human assessment of pitch. For example, the YIN algorithm and the MPM algorithm are both based upon autocorrelation.

In the frequency domain, polyphonic detection is possible, usually utilizing the periodogram to convert the signal to an estimate of the frequency spectrum . This requires more processing power as the desired accuracy increases, although the well-known efficiency of the FFT, a key part of the periodogram algorithm, makes it suitably efficient for many purposes.

Popular frequency domain algorithms include: the harmonic product spectrum cepstral analysis and maximum likelihood which attempts to match the frequency domain characteristics to pre-defined frequency maps (useful for detecting pitch of fixed tuning instruments); and the detection of peaks due to harmonic series.

To improve on the pitch estimate derived from the discrete Fourier spectrum, techniques such as spectral reassignment (phase based) or Grandke interpolation (magnitude based) can be used to go beyond the precision provided by the FFT analysis. Another phase-based approach is offered by Brown and Puckette.

Network Traffic Monitoring Using Intrusion Detection System

Dr. M. N. Yadav[1] Dr. Kezia Joseph[2] Dr. Vaibhav Meshram[3] Dr. Omprakash[4]
[1,2,3,4] Dept of ECE, Malla Reddy College of Engineering, Secunderabad, Telangana, India

Abstract— **Security is a big issue for all networks in today's enterprise environment. Many methods have been developed to secure the network infrastructure and communication over the Internet, among them the use of firewalls, encryption, and virtual private networks. Intrusion detection is a relatively new addition to such techniques. IDS protect a system from attack, misuse, and compromise. It can also monitor network activity. Network traffic monitoring and measurement is increasingly regarded as an essential function for understanding and improving the performance and security of our cyber infrastructure.**

Keywords- IDS, NTM, Pattern Matching, IMAP

I. INTRODUCTION

A. Statement Of Problem

Security is a big issue for all networks in today's enterprise environment. Intruder infect the file by adding some signatures and by applying IDS that file is detected.With networking technologies and services evolving rapidly, as witnessed by the explosive growth of the World-Wide Web, peer-to-peer networks, and the GRID, accurate network traffic monitoring is required to ensure the security and optimize the efficiency of our cyberspace.

B. Intrusion Detection System:

The purpose of the IDS is to detect certain well-known intrusion attacks on the host system and display warnings to the user and also store information regarding the IP addresses and allow the traffic based on that information.

C. Network Traffic Monitoring:

Network traffic monitoring and measurement is increasingly regarded as an *essential function* for understanding and improving the performance and security of our cyber infrastructure. Network Traffic Monitor is a network analytic tool that examines local area network usage and provides a display of upload and download statistics. The main purpose of the application is monitoring the IP traffic between your local area network and Internet.

II. LITERATURE SURVEY

A. *Basic Terminology*

1) Intrusion:

1) Host based Intrusion Detection System:

An unauthorized entry into a network or system. Frequently synonymous with an information technology security incident.

2) *Signatures:*

Signature is the pattern that you look for inside a data packet. A signature is used to detect one or multiple types of attacks Signatures may be present in different parts of a data packet depending upon the nature of the attack. Usually IDS depends upon signatures to find out about intruder activity. Some vendor-specific IDS need updates from the vendor to add new signatures when a new type of attack is discovered.

3) *Network Traffic*:

Incoming and outgoing packets generating traffic.

B. *Need*

A virus, worm program that is either downloaded from some site on the Internet, that you receive in the form of an attachment to an email message that you open, or that is delivered via an embedded Active X control or JavaScript program in a Web page. To detect these viruses and worms we need a powerful system IDS. Traffic consist of packets which are coming from various ports like HTTP,FTP,SMTP, etc; these packets may be malicious or non-malicious. To view the integrity of packets we need network traffic monitoring tool. By using network traffic monitoring tool incoming and outgoing packets are captured and then analyze by using pattern matching IDS system.

C. *Types Of Ids*

HIDS involves not only looking at the network traffic in and out of a single computer, but also checking

A New Approach to Intrusion Detection System

Dr. N. Rajesha[1] Dr. D. Kiran[2] Dr. Vaibhav Meshram[3] Dr. B. Jayachandran[4]

[1,2,3,4] Dept of ECE, Malla Reddy College of Engineering, Secunderabad, Telangana, India

Abstract: The design and implementation of intrusion detection systems (IDS) remain an important area of research in the field of security of information systems. Despite the undeniable progress, much remains to be done to improve the security of computer networks today. For this, many mechanisms have been developed {[1], [2]}. In general, these systems are vulnerable to attack from unauthorized users (external attacks) as well as attacks by authorized users (internal attacks) who abuse the privileges granted to them. In this paper, our contribution consists of the design of an intrusion detection system based on security policy at three levels. This approach, very interesting even for complex information systems, allows administrators of information systems and responsibles of network security, the protection from external attacks and internal attacks.

Keywords: *Security Policy (SP), Intrusion Detection System (IDS), Alerts Correlation (AC), Data Fusion (DF), Network Security (NS)*

1. INTRODUCTION

In recent years, significant progress has been made towards improving the security of computer systems. Unfortunately, the undeniable reality remains that all computer systems are still vulnerable. These systems are vulnerable to attack from both unauthorized users and attacks by authorized users who abuse their privileges.

In this paper, we propose an approach based on security policy at three levels for complex computer systems. These three levels working together to protect the computer system from inside and outside attacks. This global security policy will allow the administrator security systems not only to detect attacks but also to warn about this intrusion and deny access to all networks.

2. INTRUSION DETECTION SYSTEMS

2.1 DEFINITION

An intrusion detection system (IDS) is a mechanism to detect abnormal or suspicious activity on a given target to address the problems as quickly as possible. Given their practical value, the IDS have been studied heavily over the past 20 years in order to improve their effectiveness. The fruits of these studies are of different classes of IDSs that rely on different detection techniques, each of which is more appropriate for a particular context. Among others, we find the intrusion detection systems that base their decisions on information found in machines called HIDS and intrusion detection systems that base their decisions solely on information flowing in a network called NIDS. More details on the various classes of IDS and their evolution can be found in [3].

2.2 VULNERABILITY OF SYSTEMS

An attack is an exploitation of vulnerability in a system. Thus, reducing attacks can only be done with a good understanding of the system and possible sources of vulnerability in order to find suitable remedies. The word vulnerability expresses all the weaknesses of computer resources that can be exploited by malicious people. In [4], D. Denning explains the presence of vulnerabilities in information systems by, among others, the following reasons:

- ✓ Good security costs usually very expensive and most organizations do not have sufficient budget to afford this need.
- ✓ Security tools used cannot be 100% sure, see that they are often ineffective.
- ✓ Security policies are commonly complex, incomplete and sometimes inconsistent.
- ✓ The bugs in programs that are common and are still exploited by attackers.

ENHANCED PID CONTROLLER USING NEURAL NETWORKS IN MATLAB SIMULATION

G.Sridhar[1], S. Krishna Kishore[2] D. Thirupathi[3] B.C. Nirmala[4]
[1,2,3,4] Department of ECE, Malla Reddy College of Engineering, Secunderabad, Telangana, India

***ABSTRACT*:"ENHANCED PID CONTROLLER BASED ON BACK PROPAGATION NEURAL NETWORK" *is used* to tune the PID controller to update its gain automatically to its desired value. The conventional PID controller has a constant gain value where it is difficult to choose its gain if the system is a non linear system. In order to overcome this problem we are going for Adaptive PID controller based on back propagation neural network. According to the requirements of system output performance, the BP neural network can automatically adjust its weights to vary kp, ki and kd, in order to match the system. Here the system we are using is the position control system where the servo valve is used to control the position of the piston. It is called the "Electro Hydraulic Servo Valve position control system." The simulation results of an electro-hydraulic servo valve position control system using adaptive PID controller based on BP neural network shows that it can get better control characteristics adaptability and strong robustness in the nonlinear time varying system compared to correctional PID controller. At the same time, simulate results provides a theoretical basis for the design and application of electro-hydraulic position servo control system. The system here we are using is a SISO.**

Keywords: **Adaptive, Electro hydraulic system, SISO-Single input and single output system, BP-back propagation.**

1.INTRODUCTION

The proportional-integral-derivative (PID) controller is one of the most commonly used controllers in the industrial closed loop control system for its simple algorithm, good robustness and stability(fig 1). But PID controller has its disadvantage that it is not suitable for the control of long time-delay and nonlinear system, in which the P, I and D parameters are difficult to choose and can hardly adapt to time varying of characteristics in wide range. With the development of modern computer technology and control theories such as fuzzy, neural networks and gray theory these difficulties can be overcome. Back propagation (BP) is one of the neural network algorithm and is a powerful computational tool that have been used extensively in the areas of pattern recognition, systems and identification. The adaptive PID controller based on back propagation neural network which is designed combining traditional PID strategy with neural network has created a new concept and a new tool for control. The self-learning ability of BP neural network can tune automatically and modify the robust PID parameters online. Below fig shows

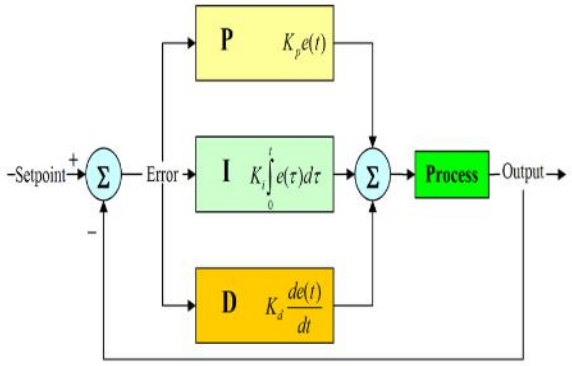


FIGURE 1: PID Controller

Where as in the case of BP neural network based PID controller. The BP identifies **kp, ki and kd** value for each instances. According to the magnitude of the error signal. Here **kp, ki and kd** values keeps on changing to improve the system performance.

Figure 2 shows the complete block diagram of the enhanced PID controller based on BP neural network. The block shows that there is an input to the system which is r.

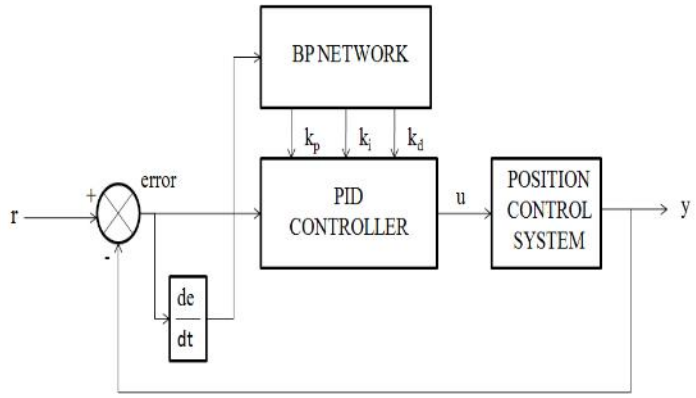


FIGURE 2: Structure of enhanced PID controller based on BP neural network.

IMPLEMENTATION OF SENSOR FUSION-BASED VACANT PARKING SLOT DETECTION AND TRACKING USING ARM-7

M. Shiva Kumar[1] B. Manjula[2] M. Suresh[3] P. Uma[4]
[1,2,3,4] Dept of ECE, Malla Reddy College of Engineering, Secunderabad, Telangana, India

Abstract- *This paper introduces an intelligent parking slot detection and tracking with ARM7-LPC2148 microcontroller. The parking problem in big cities, especially the mega-cities, has become one of the key causes of the city traffic congestion. The Vacant Parking slot detection and tracking is considered to be an effective way to improve parking situation. The parking slot occupancy classification stage identifies vacancies of detected parking slots using ultrasonic sensor data. Parking slot occupancy is probabilistically calculated by treating each parking slot region as a single cell of the occupancy grid. The parking slot marking tracking stage continuously estimates the position of the selected parking slot while the ego-vehicle is moving into it. In the experiments, it is shown that the proposed method can recognize the positions and occupancies of various types of parking slot markings and stably track them under practical situations in a real-time manner. The proposed system is expected to help drivers conveniently select one of the available parking slots and support the parking control system by continuously updating the designated target positions.*

Keywords *LPC2148, ZIGBEE, RFID READER, REFLECTION SENSORS, WIFI.*

I. Introduction

Due to the rapidly growing interest in parking aid products, automatic parking systems have been extensively researched. Target position designation is one of the primary components of automatic parking systems. This has been explored in a variety of ways that can be categorized into four types: user interface-Based, free space-based, parking slot marking based, and infrastructure-based approaches. Most of the (semi-) automatic parking system products on the market designate target positions by utilizing a user interface-based approach via a touch screen or a free space-based approach via ultrasonic sensors (usually mounted on both sides of the front bumper). Once the target position is designated, the system generates a path from the initial position to the target position and autonomously controls the steering to follow the path. For this purpose, it continuously estimates the ego-vehicle position using in vehicle motion sensor-based odometry. Meanwhile, an Around View Monitor (AVM) system has become popular as a parking aid product, and most car makers have started to produce vehicles equipped with this system. An AVM system produces a bird's-eye view image for the 360◦ surroundings of the vehicle by stitching together a number of images acquired by three or four cameras. Displaying AVM images helps drivers easily recognize parking slot markings and obstacles around the vehicle during the parking maneuver. This paper proposes a vacant parking slot detection and tracking system that fuses the sensors of an AVM system and an ultrasonic sensor-based automatic parking system. The flowchart of the proposed system is presented in Fig. 1. Once a driver starts parking, the system continuously detects parking slot markings and classifies their occupancies. Simultaneously, it presents the detection and classification results on AVM images to help the driver identify available parking slots. If a driver selects a desirable parking slot using the touch screen interface, this system tracks the position of the selected parking slot while the ego-vehicle is moving

DESIGN AND IMPLEMENTATION OF FRACTIONAL ORDER PID CONTROLLER FOR INTEGER ORDER AND FRACTIONAL ORDER THERMAL PROCESS

Dr. G.Sridhar[1] Dr. Omprakash[2] Dr. N. Rajesha[3] B. Manjula[4]

[1,2,3,4] Dept of ECE, Malla Reddy College of Engineering, Secunderabad, Telangana, India

Abstract:- **Recently, The fractional order PID control is the generalization of the PID control, has been focused. For implementation of FOPID, approximation of the fractional integrator and differentiator is required. Short memory principle (SMP) is one of the effective approximation methods. However, there is a disadvantage that the approximated filter by the SMP can't eliminate the steady state error. To overcome this, we introduce the distributed implementation of integrator technique. Using the Temperature control system of heat plate, the proposed method is implemented in MATLAB and compare it with traditional PID control scheme.**

keywords: FOPID, SMP, GL, Z-N method.

I. INTRODUCITON

The FO-PID control has a fractional integral and a differential elements in which these orders are non-integer. Generally, as the physical plant has a fractional characteristic, it is expected that the fractional controller will be effective for actual plants. There are some advantages of fractional control scheme, it was reported that $PI^{\alpha}D$ control system has a robust characteristics for the input saturation. Implementation of FOPID finite order approximation is required, fractional elements have infinite order. There have been various researches for approximation of fractional elements by the finite order filter. The SMP (short memory principle) method is effective in terms of implementation and approximation accuracy. The SMP method gives the discrete approximation of the fractional element and provides the better approximation accuracy than other digital methods. The binomial coefficients at the beginning were reduced as time advances. The integral and differential are approximated using the data during recent interval. The output error remains in steady state as the FOPID approximated by SMP.

To eliminate the steady state error, divide the fractional integral into traditional integral s^{-1} , it is called distributed implementation. The implementation method of fractional order integration, which has the integration characteristics in low frequency is examined. Approximation accuracy using SMP is evaluated.

II. PID CONTROLLER

Proportional–Integral–Derivative controller (PID controller) is a generic control loop feedback mechanism (controller) widely used in industrial control systems – a PID is the most commonly used feedback controller. A PID controller calculates an "error" value as the difference between a measured process variable and a desired set point. The controller attempts to minimize the error by adjusting the process control inputs. The PID controller calculation (algorithm) involves three separate constant parameters, and is accordingly sometimes called three-term control: the proportional, the integral and derivative values, denoted P, I, and D. These values can be interpreted in terms of time: P depends on the present error, I on the accumulation of past errors, and D is a prediction of future errors, based on current rate of change. The weighted sum of these three actions is used to adjust the process via a control element. The power supply of a heating element. In the absence of knowledge of the underlying process, a PID controller is the best controller. By tuning the three parameters in the PID controller algorithm, the controller can provide control action designed for specific process requirements. The response of the controller can be described in terms of the responsiveness of the controller to an error, the degree to which the controller the set point and the degree of system oscillation. Note that the use of the PID algorithm for control does not guarantee optimal control of the system or system stability.