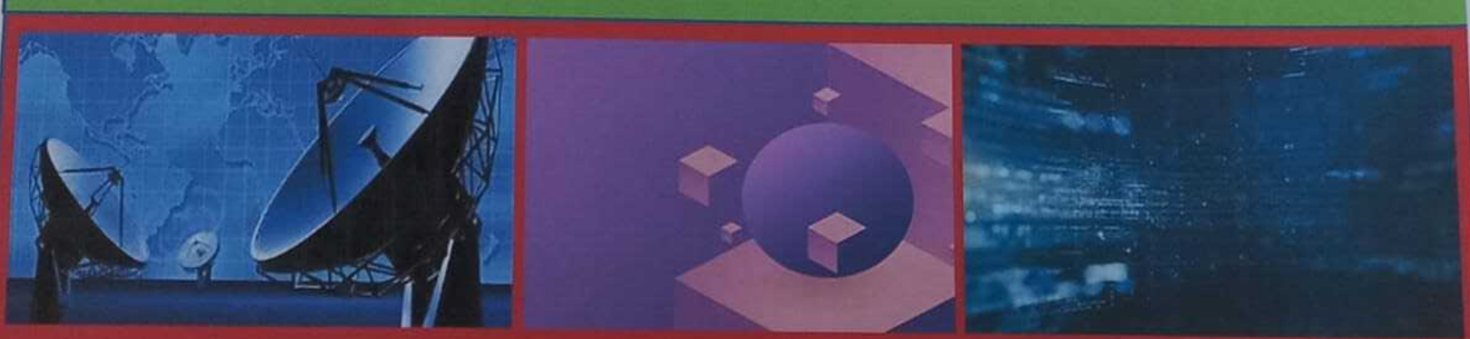
NATIONAL CONFERENCE ON ADVANCES IN COMMUNICATION ENGINEERING (NCACE-2018)

Proceedings of National Conference on Advances in Communication Engineering

(NCACE-2018)

29th & 30th August 2018



Chief Editor
Dr.Sudhanshu Sekhar Khuntia

Editor
Prof.Satya Prakash Das

GANDHI INSTITUTE OF EXCELLENT TECHNOCRATS (GIET)

www.gietbbsr.edu.in

NATIONAL CONFERENCE ON ADVANCES IN COMMUNICATION ENEGINEERING [NCACE-2018]

29th & 30th AUGUST 2018

Few Aspects of Cyber-Security Awareness: A Review

[1]**ASHUTOSH ACHARYA,**
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India
[2]**SARAT CHANDRA DASH,**
Sanjay Memorial Institute of Technology, Ganjam, Odisha, India

Abstract

The deployment of communication technologies and the use of the Internet around the world have both experienced rapid development. The major function of such technologies in daily life is information exchange. Losses arising from crimes involving the improper use of information on the Internet are on the rise. One of the Middle East's fastest-growing nations is Saudi Arabia, whose use of communication technology like the Internet and mobile devices has increased significantly in recent years. When compared to industrialised nations, the region is still developing these technologies. As a result, the crimes related to these technologies may be novel to the local populace.

1. Introduction

The scale of the rise in cybercrimes is alarming. The cost of cyber breaches in the UK alone is estimated to be £3.14 million [1]. The Business Email Compromise (BEC) scams worldwide were estimated to be more than $ 3 billion [2]. The impact of cybercrime is not just assessed solely in terms of costs incurred but also in terms of breach of data privacy which can affect many consumers. The projected losses for the businesses by the year 2019 due to cybercrime are estimated to be in the region of $2 trillion [3]. While the number of cyber security attacks in large companies has been decreasing, in medium and small sized companies it is increasing significantly, which could be a major concern for developing countries [4].

Saudi Arabia, which is one of the fastest developing countries in the Middle East, has seen enormous growth in the use of communication technologies, the Internet and mobile technologies in recent years. It is estimated that approximately 66% of the population, which equals more than 18 million users, have access to the Internet. Facebook and Twitter are used by the majority of these users [5]. About 39% of the population that uses the Internet buys products online, and the country's E-commerce business is about $520 million [6].

The penetration of the Internet and the boom in smartphone usage in KSA is relatively new.

Therefore, it can be assumed that understanding of the importance of cyber security and information on security measures which can be taken is limited.

Focusing on these aspects, a previous study investigated the cyber security awareness of the people in Saudi Arabia in different contexts. A quantitative online based survey was conducted using a survey questionnaire for gathering the information related to cyber security awareness in Saudi Arabia. The study found that though the participants have good knowledge of IT, their awareness regarding the threats associated with cybercrime, cyber security practices, and the role of government and organizations in ensuring the information safety across the Internet is very limited. The results indicated that the levels of cybercrime experiences are on the rise in recent years, and there is no specific approach being followed in the region for increasing cyber security awareness except CERT regulations, and online information on government websites. Additionally, Chi-Square test results ($t(627)=3.85$, $p=0.013$) indicated that the Internet skills have an effect on the cyber security practices from the users end, and association of the level of skills of the people with the available security measures being implemented by the responsible organizations in the region. The study has found that there is an immediate need for developing an application for creating cyber security awareness in the region in order to combat cybercrime.

Data Analytics method for Improving Cyber Security Awareness.

[1]BISWARANJAN BEHERA,
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]RAKESH CHANDRA HOTA,
Aumsai Institute of Technical Education, Berhampur, Odisha, India

ABSTRACT This article makes a modest effort to examine the problems that training and awareness programmes for cyber security face as well as the potential advantages of employing learning analytics, a developing area of data analytics, to combine existing data sources and enhance the value of these programmes. The advantages and disadvantages of implementing such programmes are not covered in this article because it was prepared with the presumption that awareness and training are effective preventive controls. Considering the expanding Internet and mobile usage in the nation, this article will discuss cyber security and cyberattacks. Participants in the prior study selected a mobile game application to deal with the issue of raising awareness. This paper covers different studies focusing on gaming applications, taking into account the findings from the prior study.

KEYWORDSawareness,compliance,cyber,dataanalytics,learninganalytics,LMS,risk

Security professionals propose that as our culture becomes more dependent oninformation,socialengineeringwillremainthegreatestthreattoanysecuritysystem.Prevention includes educating people about the value of information, training themtoprotectit,andincreasingpeople'sawarenessofhowsocialengineersoperate.

According to Wilson and Hash (2003), a cyber security education program shouldcover:

- Awareness campaigns: Optional and continual where end users decide if theywould benefit from information being transmitted. The purpose of an aware-nesspresentationissimplytofocusattentiononsecurity.Informationismostlydeliveredthroughposters, articles,rewards, andlunch-and-learnsessions.
- Training–role-based and obligatory: Management decides which end users

Advancements in Coherent Optical Fiber Communication Systems.

[1]Dr. SUDHANSHU SEKHAR KHUNTIA,
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]RAJENDRA BEHERA,
Aryan Institute of Engineering & Technology, Cuttack, Odisha, India

***Abstract*— *Coherent optical fibre communications research and development have progressed in part because to the potential for receiver sensitivity improvements up to 20 dB and in part due to the potential for frequency-division multiplexing (FDM) with extremely fine frequency separation. This study reviews current developments in coherent optical fibre communication systems research, with a focus on those that have been reported in the last two years. Four categories of bit-error rate measurements have been identified and are being investigated: PCM-ASK, PCM-FSK, PCM-PSK, and PCM-DPSK. Also covered are the most recent polarization-state stabilising approaches.*

***Index Terms*—Electrooptical modulators, lithium niobate, optical modulator, waveguide devices.**

I. Introduction

OVER THE past decade, as the demand for telecommunications services and bandwidth has boomed, the need for and advantages of external modulation in fiber-optic transmission systems has been firmly established. In higher speed digital communication applications, fiber dispersion has limited system performance. Lithium niobate ($LiNbO_3$) external modulators provide both the required bandwidth and the equally important means for minimizing the effects of dispersion. Unlike direct modulation of a laser diode, $LiNbO_3$ guided-wave modulators can be designed for zero-chirp or adjustable-chirp operation. Zero-chirp and negative-chirp modulators help to minimize the system degradation associated with fiber dispersion. In analog systems, linearized external modulators can provide very low modulation distortion.

Advances in $LiNbO_3$ modulator device technology have enabled stable operation over temperature, very low bias-voltage drift rates, and bias-free devices. These advances in device and material technology have been accompanied by significant investments in guided-wave device manufacturing. The net result today is a strong demand for and an ample supply of high-quality $LiNbO_3$ modulator components for use in fiber-optic communication systems. In this paper, we will provide an overview of the present state of $LiNbO_3$ modulator technology. More detailed and complementary information can be found in recent publications, which cover devices and system applications [1], switching technology [2], and guided-wave devices in general [3].

Section II of this paper describes the basic techniques used to fabricate $LiNbO_3$ guided-wave devices. Section III discusses various modulator device designs, structures, and functions. Section IV describes the performance of $LiNbO_3$ devices in digital systems. Section V covers some nondigital applications for $LiNbO_3$ modulators. Section VI discusses the product development cycle and manufacturability of these devices. Section VII reviews reliability data available from the field and accelerated-aging tests.

II. Device Fabrication

Lithium niobate has a very high intrinsic modulation bandwidth, but device switching speeds are limited by a variety of physical constraints. Modulation is produced by a voltage-induced change in the refractive index. The achievable index change is small and, thus, either large voltages or long electrode lengths are needed to obtain sufficient modulation. A useful figure of merit for modulation is the product of the switching voltage and the electrode length. For lengths that allow reasonable voltages, the capacitance of lumped element electrodes would limit the bandwidth to less than 1 GHz. By using travelling wave electrodes, in which the electrical signal propagates along the same direction as the optical wave, much higher bandwidths can be obtained. In this case bandwidths are limited by the mismatch between the electrical and optical propagation constants as well as by the electrical attenuation of the electrode [4]. Theoretical and experimental work has led to electrode structures optimized for 10-Gb/s digital modulation [5].

Fig. 1 depicts a cross-sectional view of an x-cut $LiNbO_3$ Mach–Zehnder interferometer (MZI) modulator, where the critical dimensions of the modulator structure are shown. Wave velocity is a function of the material properties and the waveguide cross-sectional dimensions. Because the modulator can be several centimeters long, preservation of cross-sectional dimensions along the length of a device presents a challenge not only from the standpoint of fabrication but also in the

Indoor Applications with High-Speed Optical Wireless Communication System

[1]RANJAN KUMAR SETHY,

Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]VIBHASH PATNAIK,

Aumsai Institute of Technical Education, Berhampur, Odisha, India

Abstract— *For applications involving indoor personal area networking, a unique high-speed optical wireless communication technology is proposed and investigated. With restricted mobility, a proof-of-concept experiment for 12.5Gbps wireless transmission has been successfully demonstrated. A high-speed optical wireless connection with mobility feature can be realised throughout the entire room when connected with a Wi-Fi-based localization system. Additionally analysed and measured experimentally, the performance trade-offs between the maximal beam footprint and total bit rate demonstrate that error-free (BER109) reception is always possible for a wide range of data rates from 1Gbps to 12.5Gbps.*

Index Terms— **Broadband communication, fiber optics linksandsubsystems,indooropticalwirelesscommunications,personalcommunicationnetworks.**

I. INTRODUCTION

WIRELESScommunication systems areattractivebecauseofitscapabilitytoprovidemobilitytoendusers.Comparedwiththetraditionalradiofrequency(RF)technologyand millimeter-wave systems, optical wireless (OW)technologyhasmultipleadvantages,suchastheunregulatedlargebandwidthavailable,immunitytoelectromagneticinterference,andthepossibilityoffrequencyreuseandsecurityatphysicallayerwhereopticalbeamdoesnotpenetratewallsoropaqueobjects[1].Therefore,foroveronedecadeOWcommunication for indoor applications has attracted considerableattention[2-7].

Opticalwireless (OW)communications can begeneralizedintotwogroups:thediffusedsystemandtheline-of-sight(LOS)system[2].Theformerutilizestotallydiffusedbeamthatcoverstheentireserviceareaandprovidesmobilityfunctionalitytosubscribers.However,thediffusedsystemsuffersfromseveremultipathdispersionwhichlimitsthetransmissionbitrateandalsoitisnotenergyefficient[3].Onthe other hand, the direct LOS system employs a narrow laserbeam to establish a point-to-point transmission link betweenthetransceivers;thereby thetransceiversmustbespatiallyfixed to satisfy the strict alignment requirement. Therefore nomobility can be provided in this scheme in spite of its potentialofprovidingextreme hightransmissionbitrate.

To take advantage of both kinds of OW systems, we haverecently proposed a novel OW system for indoor personal areanetworkingapplicationsandhaveexperimentallydemonstratederror-free $(BER<10^{-9})$ transmission of up to 2.5Gbps [8-10].Theconcept usedbyus is similartothe"hotspot" proposedby D.C. O'Brien et al. [4], however instead of using a separatelightsourceineach"hotspot",weproposedtheceilingmounted fiber transmitter which is simply composed by a fiberend,alensandasteeringmirror.Allthesefibertransmittersareconnectedtoacentraloffice(CO)byafiberdistributionnetwork and multiple rooms can be served by a single CO. Allthe complex functions and expensive devices are located in theCOtoreducethecost.WealsoproposedtoincorporateWiFi-based localization function with the OW system and itenablesdynamicchangeofthebeampositiontoprovideubiquitous coverage of the entire room. It should also be notedthatrecentlyaremarkable1.25GbpsindoorcellularOWcommunicationhasbeenexperimentallydemonstrated[5].However,anangle-diversityreceiverwasusedandthreetransmitters and receivers were needed for each user. In thispaper,wefurtherimproveoursystemto12.5Gbpscommunication.Wealsoexperimentallyinvestigateandquantifythetradeoffbetweenthemaximumbeamfootprintandachievablebitrateofour proposed OWsystem.

II. SYSTEMSTRUCTURE

OurproposedsystemconsistsofaCOthatcentrallyprocesses and distributes the optical signal to a number ofaccess points via an optical fiber feeder network. The CO alsoacts as a gateway to the external network. In the access point,the fiber end is the transmitter and it is incorporated with alocalization function to provide ubiquitous coverage over a4m×4m×3m room. With the localization information of thesubscriber,comparativelywiderdivergentbeamisemployedto cover that user's position and its surrounding areas. ThereforebothhighspeeddatatransmissionusingdirectLOSlinkas wellas limited mobility can be provided. When the user moves outofthatarea,whichcanbeidentifiedbythelocalizationsystem,th

A Low-Latency, High-Reliability Wireless Communication System implementation for Control Applications.

[1]RUPASHREE SAHU,

Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]BIBHUTI BHUSAN BAL,

Sanjay Memorial Institute of Technology, Ganjam, Odisha, India

***Abstract*— *Because they require low-latency, high-reliability links to maintain stability, high-performance industrial control systems with tens to hundreds of sensors and actuators use wired connections between all of their components; however, the wires cause many mechanical problems that moving to wireless links would solve. Because they are designed for either high-throughput or low-power communication between a pair or a small number of terminals, no existing or proposed wireless system can achieve the latency and reliability required by the control algorithms. A preliminary wireless system architecture that focuses on low-latency operation via reliable broadcasting, semi-fixed resource allocation, and low-rate coding is proposed. The system can handle an industrial printer application with 30 nodes in the control loop and a moderate information throughput of 4.8Mb/s.*

***IndexTerms*— Wirelesscontrol, industrialcontrol,low latency,highreliability,boundedlatency,M2M,InternetofThings,cyber-physicalsystems,wirelesssensorandactornetworks**

I. INTRODUCTION

Theexplosioninthenumberandcapabilityofmobiledevices has fueled an insatiable demand for higher data rates.Toincreasethroughputanddealwithlimitsonavailablespectrum,thegoalhasbeentomaximizethespectralefficiencyof wireless systems using information theoretic tools. Thesegains have come at the cost of secondary system parameters,suchaslatency,thatdonotfitdirectlyintoinformationtheory'sframework.Asmobiledevicesmovetowardubiquity,new andimportant applications are emerging beyond delivering high-speeddatatoindividualusers.InthevisionoftheInternetof Things, a huge number of ubiquitously distributed, mobileembedded systems and access devices will communicate bothwith each other and with the cloud. This opens the door fortruly immersive computing paradigms where wireless devicesmovebeyondonlysensingtheenvironment;theywillalsobe wirelessly connected to actuators that can manipulate thesurrounding environment. In many instances, the sensors andactuators will operate in control loops with varying degrees oflatencyrequirements(TableI)[1].

In recent years, researchers have looked at the problem ofwireless control from two angles. On the theoretical side, theyexamine how to change control algorithms to cope with thelatency introduced by communication systems, ranging fromusingamodifiedformofoptimalcontroltousingnon-uniformor event-triggered sampling [2]–[5]. On the implementationside,therehasbeeninterestindeterminingtheperformanceofcontrolsystemsusingexistingwirelessstandards[6]–[9]

Application	Latency	ErrorRate	#Nodes	Throughput
VoIP	10ms	10^{-2}	1-10	500kb/s
Smartgrid/M2M	>1s	10^{-5}	10-1000	1-100kb/s
Industrialcontrol	1-2ms	10^{-8}	10-100	5Mb/s

Digital Wireless Communication: A Review

[1]SAMARENDRA SAMAL,
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]LACHHOMOHAN MOHAPATRA,
Bajirout Institute of Engineering & Technology, Dhenkanal, Odisha, India

Abstract. Wavelets have been favorably applied in almost all aspects of digital wireless communication systems including data compression, source and channel coding, signal denoising, channel modeling and design of transceivers. The main property of wavelets in these applications is in their flexibility and ability to characterize signals accurately. In this paper recent trends and developments in the use of wavelets in wireless communications are reviewed. Major applications of wavelets in wireless channel modeling, interference mitigation, denoising, OFDM modulation, multiple access, Ultra Wideband communications, cognitive radio and wireless networks are surveyed. The confluence of information and communication technologies and the possibility of ubiquitous connectivity have posed a challenge to developing technologies and architectures capable of handling large volumes of data under severe resource constraints such as power and bandwidth. Wavelets are uniquely qualified to address this challenge. The flexibility and adaptation provided by wavelets have made wavelet technology a strong candidate for future wireless communication.

Keywords: wavelets, wireless communications, multi carrier modulation, OFDM, CDMA, cognitive radio, ultra wideband communication, wireless networks

Abbreviations: ARQ, Automatic Retransmission Query; AWGN, Additive White Gaussian Noise; BER, Bit Error Rate; BPSK, Binary Phase Shift Keying; CDMA, Code Division Multiple Access; CP, Cyclic Prefix; CR, Cognitive Radio; CWT, Continuous Wavelet Transform; DFT, Discrete Fourier Transform; DS-CDMA, Direct Sequence CDMA; DWT, Discrete Wavelet Transform; FCC, Federal Communications Commission; FDM, Frequency Division Multiplexing; FDMA, Frequency Division Multiple Access; GI, Guard Interval; HiperLAN, High Performance Radio Local Area Network; ICI, Inter-Carrier Interference; IOTA, Isotropic Orthogonal Transform Algorithm; IR, Impulse Radio; ISI, Inter-Symbol Interference; LDPC, Low-Density Parity-Check; MANET, Mobile Ad hoc Networks; MB-OFDM, Multi-Band OFDM; MC-CDMA, Multicarrier CDMA; MC-DS-CDMA, Multicarrier Direct Sequence CDMA; MCM, Multicarrier Modulation; OFDM, Orthogonal Frequency Division Multiplexing; OWDM, Orthogonal Wavelet Division Multiplexing; PAM, Pulse Amplitude Modulation; PAPR, Peak-to-Average Power Ratio; PR, Pseudo Random; PR-QMF, Perfect Reconstructed Quadrature Mirror Filter; PSWF, Prolate Spheroidal Wave Functions; PSD, Power Spectral Density; PSK, Phase Shift Keying; QAM, Quadrature Amplitude Modula- tion; QMF, Quadrature Mirror Filters; QoS, Quality of Service; QPSK, Quadrature Phase Shift Keying; SCDMA, Scale Code Division Multiple Access; S-CDMA, Synchronous Code Division Multiple Access; SNR, Signal-to- Noise Ratio; SSA-UWB, Soft Spectrum Adaptation UWB; STCDMA, Scale Time Code Division Multiple Access; TDM, Time Division Multiplexing; TDMA, Time Division Multiple Access; TDOA, Time Difference Of Arrival; UWB, Ultra Wideband; V-BLAST, Vertical Bell Laboratories Layered Space Time; WP, Wavelet Packet; WPM, Wavelet Packet Modulation; WDM, Wavelet Division Multiplexing; WDMA, Waveform Division Multiple access; WPDM, Wavelet Packet Division Multiplexing; WPT, Wavelet Packet Transform

1. Introduction

The Wavelet transform is a way of decomposing a signal of interest into a set of basis waveforms, called wavelets, which thus provide a way to analyze the signal by examining the

Optimization of Urban Optical Wireless Communication Systems

[1]SANKARSAN SAHU,

Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]YASHOWANTA NARAYAN DIXIT,

Aryan Institute of Engineering & Technology, Cuttack, Odisha, India

***Abstract*— *Optical wireless communication systems in cities are regarded as a "last mile" technology. The atmosphere is used as a propagation medium in an optical wireless communication system. The transceivers are mounted on high-rise buildings to provide line-of-sight (LOS). Buildings sway, however, due to dynamic wind loads, thermal expansion, and minor earthquakes. To maintain LOS between the transmitter and the receiver, the designer must increase the transmitter beam divergence angle. An excessively wide divergence angle clearly increases the required laser power and, as a result, terminal cost and complexity. When there is building sway, an overly narrow beam divergence angle may result in communication cutoff. We develop a mathematical model in this paper.*

***Index Terms*—Building sway, optical communication, optimiza-tion, wireless communication.**

I. Introduction

IN THE communication world, urban optical wireless communication (UOWC) is one of the major areas that remain to be comprehensively researched. UOWC uses light beams propagating through the atmosphere to carry information (Fig. 1). The UOWC terminal includes an optical transmitter and a receiver, both of which are placed on high-rise buildings at a separation distance of several hundred meters. The main advantages of UOWC are: 1) there are no licensing requirements or tariffs for its utilization; 2) there is no need to dig up roads, etc.; 3) it enables very high data rates; and 4) it is small, light, and compact. However, a problem that has to be dealt with is that under the influence of dynamic wind loads, thermal expansion, and weak earthquakes, typical high-rise buildings sway. The building sway causes vibrations of the transmitter beam moving it from the line-of-sight (LOS) in the direction of the receiver. These vibrations decrease the average received signal, which in turn, increases the bit-error probability (BEP). Hence, the designer is required to increase the transmitter beam divergence angle and power so as to maintain LOS between the transmitter and the receiver. It is clear that an overly wide divergence angle will increase the required laser power, which increases the terminal cost and complexity. On the other hand, an overly narrow beam divergence angle may result in cutoff in communication when there is building sway.

The theory of optical wireless communication (OWC) is presented in [1] and [2]. The effects of wind, earthquakes, and thermal expansion on an OWC system are described in Kim *et al.* [3]. Acampora *et al.* [4] proposed a hybrid access network that uses small radio cells, where the cell base stations are interconnected by optical wireless links. The effect of fog on the bit-error rate of a free-space laser communication system is presented in [5]. A simple method to evaluate the performance of mesh networks as a function of weather attenuation is proposed by Kaneko *et al.* [6]. A new technology to mitigate weather attenuation using quantum cascade lasers at far infrared wavelengths is demonstrated by Capasso *et al.* [7]. Turbulence and pointing error effects on OWC link performance are analyzed in [8] and [9]. Two error probabilities are commonly used in space laser communication: the BEP [10], [11] and the burst-error probability [12]. An evaluation and comparison of seven of the world's major building codes and standards with specific discussions of their estimations of the alongwind, acrosswind, and torsional response is given in [13].

In this paper, we develop a BEP model that takes into account building-sway statistics and communication system parameters. We assume that the receiver has knowledge about the marginal statistics of the signal fading and the instantaneous signal fading state. Then we derive a mathematical model to minimize transmitter power and optimize transmitter gain (the divergence angle) for a given BEP. For example, for a BEP of 10^{-9}, we achieve at least a 4-dB reduction of the required transmitter power in comparison to a system with both half and twice the optimum beam divergence angle. This reduction in laser power could improve the overall system performances and cost considerably.

The remainder of this paper is organized as follows. In Section II, we present the building-sway model. Section III oulines the communication system model in preparation for a description of the optimization procedure. We conclude with a discussion of the practical implications of this study.

II. Building Sway

Building sway can be caused by strong winds, thermal expansion of building frame parts, and earthquakes [3]. Under the influence of dynamic wind loads, typical high-rise buildings sway in the alongwind, acrosswind, and torsional directions [13]. The alongwind motion primarily results from pressure fluctuations on the windward and leeward faces, which

Sharing the Spectrum in Radar and Wireless Communication Systems

[1]SATYA PRAKASH DAS,
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]BINOD KUMAR SAHOO,
Aumsai Institute of Technical Education, Berhampur, Odisha, India

Abstract — *The concept of sharing spectrum between radar and wireless communication systems arose as a result of the need for additional bandwidth for wireless communication systems. The realisation of this vision is unavoidable in the near future due to strong and ever-increasing economic, political, social, and technological driving factors. As a result, novel solutions for efficient and equitable spectrum sharing are required. We present a concise review of the state of the art in radar and communication system coexistence and bandwidth sharing in this paper.*

1 INTRODUCTION

Wireless communication technology has recently evolved dramatically with ever growing number of users and proliferation of applications, that it become a indispensable feature of human life [1]. With increasing number of mobile devices and demands on higher data transmission rates for advance wireless technology, more radio spectra are sought after by commercial service providers and federal agencies [2]. The demand on radio spectrum urges efficient use of spectrum and emerges a challenging problem on future spectrum planning. In [1], it is clearly addressed that new Federal spectrum architecture should be based on sharing rather than clearing and reallocating the sought after spectrum. Thus, spectrum sharing technology has emerged as a developing research topic to both radar and communication communities. Hence, cooperation between these two established technology areas needs to be vitalized and extended. In this paper, we present a concise review of the state of the art on radar and communication system coexistence and bandwidth sharing.

2 SPECTRUM SHARING CONSIDERA-TIONS

Spectrum sharing, or shared spectrum access, involves a primary user, whom the bandwidth is licensed to, and a secondary user that utilizes the same spectrum band without endangering any mission of both sides [3]. Until recently, spectrum allocation (*i.e.*, a certain frequency band is assigned exclusively to a certain electromagnetic wave emitting technology like radar or wireless communications) was vital to prevent any interference among different systems. However, with the emergence of recent technologies in radio communication, spectrum sharing in time and space has a feasible future [4]. In particular cognitive radio is an emerging technology that can exploit unused/underutilized spectrum bands via opportunistic dynamic spectrum sharing [5].

Technical challenges of spectrum sharing involves both accurately sensing radio environment, and transmitting signals accordingly. Challenges of spectrum sharing in communication systems are widely investigated in numerous studies [6–10]. Although, the effects of RF interference in radar systems concerning spectrum sharing is investigated in the past (*e.g.*, [11]), more work needs to be done to understand drawbacks and fundamental limits of spectrum sharing in radar and communications systems coexistence.

3 SPECTRUM SHARING TECHNIQUES AND APPROACHES

Shared spectrum access for radar and communications is one of the important research and development areas which is identified by DARPA [12]. In fact, the solutions for spectrum sharing can be classified into three broad categories. In the first category, radar system as taken as the primary user and the objective is the maximize the performance of the communication system utilizing radar spectrum as a secondary user (*i.e.*, radar performance should not be deteriorated by the communication system). In this category radar system is not affected by the shared use of the spectrum and the burden of ensuring this constraint is on the communication system, entirely. In the second category, solutions are proposed to mitigate the interference caused by the communication system on the radar. Although it is assumed the communication system is operating cognitively, the proposed solutions are developed by assuming the interference

Wireless channel estimation and jamming-resilient communication for Smart Grid with Rechargeable Electric Vehicles.

[1]SRIRAM PRADHAN,
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]PRATIK PATTANAYAK,
Aryan Institute of Engineering & Technology, Cuttack, Odisha, India

ABSTRACT

Current transportation systems emit significant amounts of greenhouse gases into the atmosphere. Recent advances in fuel cell battery technology are making zero-carbon electric vehicles (EVs) more practical for the commercial market. However, widespread adoption of EVs necessitates the support of a powerful and resilient power grid capable of efficiently generating, aggregating, and distributing a large amount of energy in real time while emitting little carbon. Such a system necessitates the use of modern communication technologies, which are vulnerable to various cyber attacks. Attacks on the smart grid communication system can have catastrophic consequences for the highly interdependent smart grid users. In this article, we first propose a smart grid model for mass EV use, and then discuss some common security concerns.

INTRODUCTION

To restrict the increment of global temperature to 2°C, carbon emission has to be cut by 50 percent by 2050 compared to the emission in 1990. Research results published by Allen *et al.* show that to satisfy this goal, the total CO_2 emission should not exceed 1000 billion by 2050 [1]. However, by the end of the first decade of this century, one third of this budget had been used up. A low-carbon society cannot merely be a scene in science fiction. A real transition from a high-carbon-emission society to a zero-carbon one must happen in order to save the world from global warming.

A potentially reducible greenhouse gas source is the carbon fuel used in transportation systems. Transportation contributes to more than 27 percent of the total CO_2 emission in the United States [2]. The space for emission reduction is appealing. The current advances in fuel cell battery technologies make commercial electric vehicles (EVs) possible in the near future. However, the prevalence of EVs imposes a challenge on load balancing in the power grid. This is because to achieve desirable usability of the EVs, a large charging current is required to shorten the charging time. Such demand incurs heavy load on the power grid when mass EVs are charging simultaneously. Moreover, the unbalanced and dynamic distribution of car charging events calls for a power system that is highly resilient to huge load fluctuations. For example, unprecedented peak hours can appear to be regular nightmares for the power grid each night when most of the cars are charging. And the cars may charge at parking lots of workplaces during the day and at residential areas at night. Such geographical variation in load largely disturbs the load balancing of the power grid.

Recently, smart grid technology has been proposed to improve the efficiency and safety of the power grid [3]. The widespread adoption of EVs inherently relies on the interaction between the individual EV and the smart grid. The bond connecting them is ubiquitous communication networks. Such a network for smart grid is built on open or heterogeneous system architecture [4], which incorporates all the modern communication technologies. At the architectural level, many instruments, sensors, controllers, and management computers are interconnected and accessible through the Internet. At the technical level, Zigbee networks, WiFi networks, WiMAX networks, and cognitive radio networks are all feasible for supporting the information collection and communication in various application scenarios in the smart grid. A conceptual example of the smart grid with ubiquitous communications is shown in Fig. 1.

Although arming the power grid with various communication technologies enhances the flexibility and efficiency of the power grid, the vulnerabilities that inherently reside in these communication systems transform into security risks in the power infrastructures. In this article, we first introduce the cyber security threats against the smart grid with EVs, then focus on two wireless security techniques for secure communication between the EVs and the smart grid.

Implementation of Wireless Power Supply System in Industrial Automation Systems

[1]ARPITA SWAIN,
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]PRAKRITI PATNAIK,
Bajirout Institute of Engineering & Technology, Dhenkanal, Odisha, India

***Abstract*— We have seen significant advances in low power, integration, and micro-systems technologies in recent years, enabling wireless communication for very small, affordable, lightweight, and high performance devices. These technologies are still primarily used for consumer and office applications, but they can provide significant benefits when applied to new areas. Industrial automation and control systems, such as robotics and factory automation, are of particular interest. In this paper, we discuss the main challenges of developing a reliable, wireless, and energy-efficient communication system for industrial automation. Special emphasis is placed on providing an overview of suitable power supply options as well as describing a novel magnetic medium frequency power supply concept that enables true wireless energy supply within cell-volumes of more than loom' with.*

***Index Terms*—Cross-layer design, industrial wireless sensor networks (IWSNs), ISA100, ultrawideband (UWB), wireless HART, ZigBee, 6LoWPAN.**

I. Introduction

IN TODAY'S competitive industry marketplace, the companies face growing demands to improve process efficiencies, comply with environmental regulations, and meet corporate financial objectives. Given the increasing age of many industrial systems and the dynamic industrial manufacturing market, intelligent and low-cost industrial automation systems are required to improve the productivity and efficiency of such systems [6], [28]. Traditionally, industrial automation systems are realized through wired communications. However, the wired automation systems require expensive communication cables to be installed and regularly maintained, and thus, they are not widely implemented in industrial plants because of their high cost [29]. Therefore, there is an urgent need for cost-effective wireless automation systems that enable significant savings and reduce air-pollutant emissions by optimizing the management of industrial systems.

With the recent advances in wireless sensor networks (WSNs), the realization of low-cost embedded industrial automation systems have become feasible [2]. In these systems, wireless tiny sensor nodes are installed on industrial equipment and monitor the parameters critical to each equipment's efficiency based on a combination of measurements such as vibration, temperature, pressure, and power quality. These data are then wirelessly transmitted to a sink node that analyzes the data from each sensor. Any potential problems are notified to the plant personnel as an advanced warning system. This enables plant personnel to repair or replace equipment, before their efficiency drops or they fail entirely. In this way, catastrophic equipment failures and the associated repair and replacement costs can be prevented, while complying with strict environmental regulations.

The collaborative nature of IWSNs brings several advantages over traditional wired industrial monitoring and control systems, including self-organization, rapid deployment, flexibility, and inherent intelligent-processing capability. In this regard, WSN plays a vital role in creating a highly reliable and self-healing industrial system that rapidly responds to real-time events with appropriate actions. However, to realize the envisioned industrial applications and, hence, take the advantages of the potential gains of WSN, effective communication protocols, which can address the unique challenges posed by such systems, are required.

Due to unique characteristics and technical challenges, developing a WSN for industrial applications requires a combination of expertise from several different disciplines [9]. First of all, industrial expertise and knowledge are required for application-domain-specific knowledge. Second, sensor-technology expertise is essential to fully understand issues associated with sensor calibration, transducers, and clock-drift. Third, RF design and propagation environment expertise is necessary to address communication challenges and RF interference problems in industrial environments [31]. Finally, networking expertise is needed for understanding the hierarchical network architectures and integrating different networks, which are required for industrial WSNs (IWSNs) to provide flexible and scalable architectures for heterogeneous applications.

Recently, many researchers have been engaged in developing schemes that address the unique challenges of IWSNs. In this paper, first, technical challenges and design principles are introduced in terms of hardware and software developments and system architecture and protocol design. Specifically, radio technologies, energy-harvesting techniques, and cross-layer design for IWSNs are discussed. In addition, IWSN standards

Charging Time Control of Wireless Power Transfer Systems

[1]ASHOK BABU,
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]SATYAJIT MOHAPATRA,
Barunei Institute of Engineering and Technology, Khordha, Odisha, India

Abstract— *It is presented a charging time control method for wireless power transfer systems with secondary-side hysteresis output power control. It is a primary-side control method that employs the combined use of three concepts, namely I an intermediate capacitor in the receiver circuit as a power flow indicator, (ii) the hysteresis switching actions of a shunt decoupling power switch in the receiver circuit to regulate the DC voltage of such intermediate capacitor, and (iii) the primary-side turn-on and turn-off times of the decoupling switch for closed-loop control. This method eliminates the need for I precise information of the mutual inductance between the transmitter and receiver coils, as well as (ii) a wireless communication system for feedback purposes.*

***Index Terms*—Wireless power transfer (WPT), primary-side control**

I. Introduction

WIRELESS power transfer (WPT) systems have attracted lots of attentions in research communities and industry in the last two decades. Recent research efforts reported in the literature focus on several major applications, including wireless charging of (1) mobile robots [1], (ii) consumer electronics [2] and (iii) medical implants [3-5]. Applications of WPT face a common issue of the need for a mechanism for monitoring the output load conditions for feedback purposes. For wireless charging of portable consumer electronics, for example, the relative positions of the *Tx* coil and the *Rx* coil may not be fixed precisely. Any WPT application requires the receiver circuit to be physically separated from the transmitter circuit. For good power control in the receiver circuit, there is aneed for some form of feedback control. In general, control executed in the transmitter circuit is called the primary-side control. Primary-control methods for WPT systems can be classified into the following groups:

(i) Use of primary side control that requires ***wireless communication systems*** [6]-[8] to feed information obtained from the receiver circuit back to the transmitter circuit for closed-loop control (Fig. 1).

(ii) Use of primary (transmitter) control that requires information of the ***mutual coupling (k) or mutual inductance (M)*** [9]-[13] between the *Tx* and *Rx* coils.

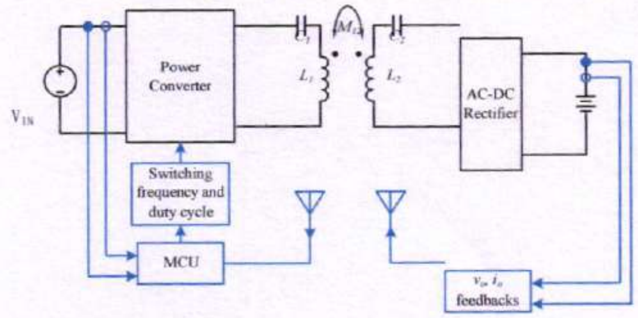


Fig. 1. Primary control of a wireless power transfer system using a wireless communication system for feedback purpose [8].

The second group of primary-side control methods that require the information or estimation of the mutual inductance (M) or mutual coupling (k) between the *Tx* coil and the *Rx* coil can be found in the references [9]-[13]. In general, they either use pre-determined value of M or estimate the value of M so that the output voltage can be calculated from information available on the transmitter (primary) side.

In this paper, a method that eliminates the needs for both of the mutual coupling information and wireless communication system for feedback control is proposed. It is based on the combined use of several concepts, including (i) an intermediate capacitor in the receiver (secondary) circuit as a power flow

Wireless Communication System with Legendre-FLANN-based Nonlinear Channel Equalization

[1]BAKDEVI SARANGI,
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]SIDDHARTH PATTNAIK,
Bajirout Institute of Engineering & Technology, Dhenkanal, Odisha, India

***Abstract*— We present the findings of our research on the use of artificial neural networks (ANNs) for adaptive channel equalisation in a digital communication system using a 4-quadrature amplitude modulation (QAM) signal constellation. We propose a novel single-layer Legendre functional-link ANN (L-FLANN) that expands the input space into a higher dimension using Legendre polynomials. Extensive computer simulations were used to compare the performance of various ANN-based equalisers, including the radial basis function (RBF), Chebyshev neural network (ChNN), and the proposed LFLANN, as well as a linear least mean square (LMS) finite impulse response (FIR) adaptive filter-based equaliser. The mean square error (MSE), bit error rate (BER), and computational complexities of the various architectures, as well as the eye, are performance indicators.*

***Keywords*—Legendre functional link artificial neural network, nonlinear channel equalization.**

I. Introduction

In wireless communication systems, transmission bandwidth is one of the most precious resources. To make efficient utilization this resource signals are usually transmitted through band-limited channels. Some of the inherent properties of the frequency-selective channels are that they are nonlinear and dispersive, and possess long delay spread. Due to these properties, the channel introduces inter-symbol interference (ISI) which reduces the data transmission rate. If the duration of the transmitted pulse is much smaller than the multipath delay spread, then each of the multipath components cannot be resolved in time at the receiver. Therefore, the currently transmitted pulse interferes with the previously and subsequently transmitted pulses, resulting in undesirable ISI and irreducible error floors at the receiver end of digital communication systems [1].

To mitigate the adverse effects of nonlinear channels, usually channel equalization is carried out in the digital system. Equalization refers to signal processing technique used at the front-end of the receiver to combat ISI in dispersive channels in the presence of additive noise. Traditionally, linear adaptive filters (AFs) are used to implement the equalizer. However, the performance of AF equalizers severely deteriorates when the channel is nonlinear and highly dispersing [2]. Therefore, in order to improve the performance of equalizers in nonlinear channels, new equalizer structures are needed.

Artificial neural networks (ANNs) can perform complex mapping between its input and output space and are capable of forming complex decision regions with nonlinear decision boundaries [3]. Further, because of nonlinear characteristics of the ANNs, these networks of different architectures have found successful application in channel equalization problem. Siu *et al.* [4] proposed a multilayer perceptron (MLP) structure for channel equalization with decision feedback and have shown that the performance of this network is superior to that of a linear equalizer trained with LMS algorithm. A radial basis function (RBF)-based equalizer structure with satisfactory performance has been reported [5]-[6].

The functional link-ANN (FLANN) is first introduced by Pao [7]. In FLANN, the original input pattern undergoes a pattern enhancement by using some nonlinear functions. Then the enhanced patterns are applied to a single-layer perceptron. Due to the absence of hidden layers, the computational complexity of FLANN is drastically reduced. In order to reduce the computational complexity, efficient functional-link ANN (FLANN)-based equalizer structures have been proposed [8]-[9]. The functional expansion in these networks was carried out using orthogonal trigonometric functions. Recently, a reduced-decision feedback FLANN channel equalizer is also proposed [10]. Another computational efficient network, i.e., Chebyshev neural network (ChNN) has been proposed for pattern classification [11], functional approximation [12], nonlinear dynamic system identification [13]-[14] and nonlinear channel equalization [15]. In these networks the expansion of input pattern is carried out using Chebyshev polynomials. ChNN provides similar, and in some cases, better performance than an MLP network but with much reduced computational load.

Similar to ChNN, the Legendre function-based neural networks, i.e., Legendre functional-link ANN (L-FLANN), provides computational advantage while promising better performance. In this paper, we propose a novel L-FLANN based nonlinear channel equalization technique. By taking several channels and different nonlinearities, with extensive simulations we have shown the effectiveness of the L-FLANN-based equalizer. We have shown that the proposed equalizer performs much better than the RBF-based and a linear FIR-based equalizers. However, its performance is similar to that of

A futuristic approach for Mobile Communication System towards Year 2020

[1]BIBHUPRAKASH PATI,
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]TEJASWI NARAYAN DIXIT,
Barunei Institute of Engineering and Technology, Khordha, Odisha, India

The forecast for future traffic demand over the next ten years shows an increase in 1000 scales and more than 100 billion Internet of Things connections, posing a significant challenge for future mobile communication technology beyond the year 2020. When it comes to enabling a connected mobile world, the mobile industry is struggling with the challenges of high capacity demand but low cost for future mobile networks. 5G is expected to shed light on these contradictory demands by 2020. This paper first forecasts the vision of mobile communication's application in society's daily life, and then figures out traffic trends and demands for the next 10 years from the perspective of Mobile Broadband (MBB) service and Internet of Things (IoT), respectively.

1. Introduction

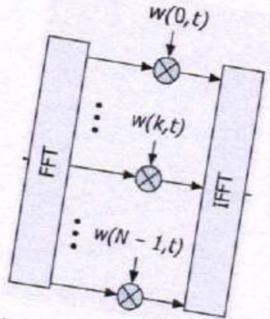
The first generation of mobile communication system based on analog signal was born in the 1980s, and it helped people get rid of the shackles of telephone line. In the 1990s more efficient second-generation (2G) mobile communication systems based on digital communication occurred, and after that personal mobile communications have had a rapid development on a global scale. After 2000, with the deployment of 3G systems, people can enjoy faster mobile Internet experience, such as video telephony. When it comes to 2010, deployment of Long Term Evolution (LTE) based 4G commercial network further enhanced the system capacity and user experience. According to the statistics of Global TD-LTE Initiative (GTI), 364 LTE commercial networks have been launched by the third quarter of 2015. The evolution map of mobile communications since 1980s is summarized in Figure 1. With the IMT-Advanced (IMT-A) systems being deployed in the world, the 5th-Generation (5G) mobile communication technologies are emerging into research fields.

In order to drive future development of mobile communication techniques, the METIS (Mobile and Wireless Communications Enablers for the Twenty-Twenty Information Society) project [1] of European Union started research work of 5G at the end of 2012. In China, IMT-2020 promotion group was founded in April of 2013. IMT-2020 promotion group will serve as a platform to promote the 5G study. Its target is to organize domestic forces to actively carry out international cooperation and to jointly promote the international development of 5G. In Korea, Samsung tested and verified the technical feasibility of millimeter wave in the bands of about 28 GHz [2]. Other possible candidate technologies such as massive MIMO [3], novel multiple access [4], and new channel coding [5–7] have attracted more and more interest. The International Telecommunication Union (ITU) has also started its study on the International Mobile Telecommunication system towards 2020 (IMT-2020) since 2013 [8]. Third Generation Partnership Project (3GPP) will start its study and standardization work on IMT-2020 from March 2016 [9].

Performance analysis of CDMA-OFDM for mobile communication system

[1]KABITA MANJARI SAMAL,
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]UNMESH SAHOO,
Sanjay Memorial Institute of Technology, Ganjam, Odisha, India



A very high-speed wireless access of 100 Mb/s to 1 Gb/s is required for 4G systems. However, for such high-speed data transmissions, the channel is severely frequency-selective due to the presence of many interfering paths with different time delays. CDMA is a promising wireless access technique that can overcome channel frequency selectivity.

Abstract

The OFDM technique is an intriguing approach in mobile communications for achieving high spectral efficiency and combating channel frequency selectivity. A CDMA system with a Rake-receiver is another intriguing technique. Although the primary benefits of CDMA are well known, its capacity is limited by multiuser interference. The goal of this research is to combine the CDMA system principle with OFDM. This combination enables maximum-likelihood detection (MLD), efficient spectrum utilisation, frequency diversity, and the retention of many CDMA system advantages. Furthermore, it enables simple cell separation via frequency hopping and a simple hardware implementation. Two examples of CDMA/OFDM mobile communication systems with Walsh-Hadamard codes.

Introduction

Wireless or cellular mobile communications systems have been evolving according to advancements in wireless technologies and changes in user demands. In fixed and cellular networks, voice conversation was the dominant service for a long time. In line with the recent explosive expansion of Internet traffic in fixed networks, demands for broad ranges of services are becoming stronger even in mobile communications networks. A variety of services are now available over the second-generation (2G) mobile communications systems, including email, Web access, and online services ranging from bank transactions to entertainment, in addition to voice conversation. People want to be connected anytime, anywhere with the networks, not only for voice conversation but also for data conversation (i.e., downloading/uploading information). 3G systems based on wideband direct sequence code-division multiple access (DS-CDMA) [1], with much higher data rates of up to 384 kb/s (around 10 Mb/s in the later stage), were put into service in some countries, and their deployment speed has since accelerated. However, the capabilities of 3G systems will sooner or later be insufficient to cope with the increasing demands for broadband services that will soon be in full force in fixed networks. Demands for downloading of ever increasing volumes of information will become higher and higher. 4G systems that support extremely high-speed packet services are now expected to emerge around 2010 [2]. How cellular systems have evolved from 1G to 3G and will further evolve into 4G is shown in Fig. 1. 100 Mb/s~1 Gb/s class wireless packet access may be necessary for 4G systems.

In this article we focus on CDMA for 4G systems. Before discussing CDMA, the propagation channel is introduced for better understanding of the frequency-selective channel. Then two approaches to CDMA are introduced: DS-CDMA and multicarrier (MC)-CDMA [3, 4]. Both DS- and MC-CDMA have the flexibility to provide variable rate transmissions, yet retain multiple access capability. Frequency domain equalization (FDE) is a key technique for both CDMA approaches. Since a major transmission mode in 4G systems will be packet-based, we also introduce automatic repeat request (ARQ) combined with channel coding.

Characterization of Broadband Channel

There are several large obstacles between a base station (BS) and a mobile station (MS), and also many local scatterers (e.g., neighboring buildings) in the vicinity of the MS. Reflection of the signal by large obstacles creates propagation paths with different time delays; each path is a cluster of irresolvable multipaths created by reflection or diffraction, by local scatterers, of the transmitted signal reaching the surroundings of an MS. They interfere with each other, producing multipath fading, and the received signal power changes rapidly in a random manner with a period of about half-carrier wavelength when the MS moves. Such a multipath channel can be viewed as a time varying linear filter of impulse response $h(\tau, t)$ observed at time t, which can be expressed as [5]

$$h(\tau,t)=\sum_{l=0}^{L-1}\xi_l(t)\delta(\tau-\tau_l), \qquad (1)$$

4th Generation Mobile Communication System: A Review

[1]LUSI DALAI,

Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]PABITRA MOHAN JENA,

Bajirout Institute of Engineering & Technology, Dhenkanal, Odisha, India

Abstract— *To meet users' expectations for more advanced wireless access even in mobile environments, research and development efforts for the Fourth Generation (4G) mobile communication system have been discussed. This paper describes the system requirements, technical challenges to be overcome, and activities related to the standardisation of the 4G mobile communication system.*

4G mobile communication system; standardization

I. INTRODUCTION

The users of the Third-Generation (3G) International Mobile Telecommunications-2000 (IMT-2000) [1] mobile communication services, which was launched in October 2001, has already reached about 34 million subscribers in Japan. The system provides a variety of advanced multimedia services such as video communications and high speed internet access. It is expected that this will lead to the mobile communication more important to our daily lives and will expand the role as a lifestyle basis in the next ten years. It is also expected that such an era requires a more advanced wireless communications system, such as the Fourth-Generation (4G) mobile communication system, which far surpasses the capability of the existing IMT-2000 as shown in Figure 1. The development process of the new mobile systems consists of developing the requirements, providing solutions satisfies the requirements, showing evidences for each technology to satisfy the requirements, as well as building international consensus through the standardization activities. In this article, we describe a basic approach to the technical issues and system configuration involved in achieving the capability and performance required of the 4G system. We also describe the trends in standardization concerning mobile communication systems.

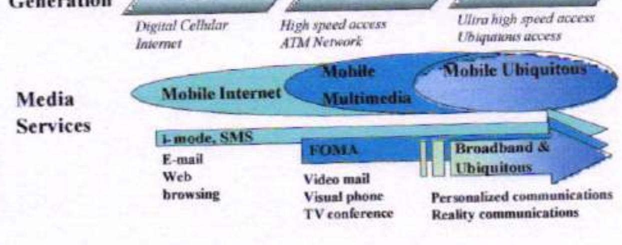


Figure 1 Evolution of the Mobile Communications Systems

II. SYSTEM OBJECTIVES

A. *Applications for 4G systems*

The improvements in media communication quality have been one of the most perceptible advancements and only the perceptible advancements noted by the customers. For example, the size and resolution of LCD (Liquid Crystal Display) screens, the number of pixels in built-in camera, and the wide variety of ringer tones have been key to the popularity of mobile handsets. However, current mobile terminals still have much room in terms of improving communication reality. The ultimate objective of enhanced-reality media communications is to provide a transparent environment that is indistinguishable from face-to-face communications.

The applications, which require more advanced wireless capabilities, are discussed in [2]. In the article, three main directions for enhancing media communication reality, that is 3D audio communications, 3D visual communications and biological information communications, as shown in Figure 2, were analyzed, and as a conclusion, it is expected that the future customers will be able to full use of 1 Mbit/s to 100

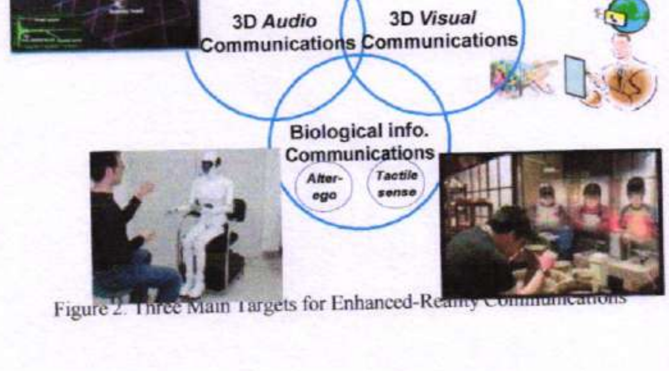


Figure 2. Three Main Targets for Enhanced-Reality Communications

Analysis of an OFDM-TDMA Mobile Communication System

[1]SARAJIB BANERJEE,
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]PREETAM BAL,
R K Institute of Engineering & Technology, Cuttack, Odisha, India

Abstract— *The multicarrier transmission technique (OFDM) is investigated in this paper in conjunction with a TDWDD multiple access scheme for a cellular mobile communication system. The performance analysis for the uncoded and coded (TCM) cases is presented. It is demonstrated that OFDM systems have a large potential for flexible allocation of the total available bandwidth to different users. This adaptability can be used to compensate for radio channel impairments, improving overall performance. Two methods are investigated, namely (1) the simple principle of leaving out weak subcarriers and (2) individual modulation of each subcarrier (adaptive modulation), with results in terms of throughput and BER performance discussed.*

Index Terms—**Cochannel interference, flat and frequency-selec- tive fading channels, orthogonal frequency-division multiplexing,smart antennas, wireless communication systems.**

I. Introduction

FUTURE wireless communications systems will need to be able to support a high level of user traffic along with a wide range of high-quality services that not only include high-quality voice but also data, facsimile, still pictures, and video. Providing these high-quality services over the harsh wireless channel with a limited spectrum implies that an increase in the capacity of current wireless systems will need to be achieved [1]–[4]. One possible approach to increase system capacity is through the use of smart or adaptive antennas [5], [6] that make use of spatial diversity to compensate for channel impairments without increasing the transmitted power or bandwidth.

With recent developments in hardware miniaturization and advances in antenna design [7], smart antennas at both the base (BS) and mobile stations (MS) have been suggested to achieve further increases in capacity as well as performance [3], [8], [9], [11]. The generalized problem of coded modulation with multiple transmit and multiple receive antennas has been addressed [3] while Raleigh and Cioffi [8] studied space-time water-filling for multipath fading, with prior knowledge of the channel. In [9], Kohno considered the maximization of signal-to noise ratio (SNR) by a joint multiple transmission and reception filters system. However, cochannel interference (CCI) has not been considered in any of these previous studies. Recent works by Lu *et al.* [10] and Wong *et al.* [11] have investigated the joint use of smart antennas at the BS and MS for performance improvement. In [10], zero-forcing based transmit antenna weights and minimum mean-square-error (MMSE) receive antenna weights are proposed for multichannel communication systems, but the subchannel gains can be arbitrarily small since the weights at the transmitter and receiver are not jointly optimized. Recently, the joint optimal antenna weights at both the BS and MS have been derived for interference-limited fading channels [11]. Nevertheless, large system complexity and/or degradation of system performance occurs in frequency-selective fading channels.

In this paper, we investigate the performance of the smart base and smart mobile (SBM) antennas discussed in [11] in conjunction with orthogonal frequency-division multiplexing (OFDM) [12], and we will refer to this combined SBM and OFDM system as SBM/OFDM. This approach utilizes the CCI rejection capability of the smart antennas and the intersymbol interference (ISI) rejection capability by OFDM. Hence, multiple users can be accessed in space, time, and by subcarriers. Therefore, one may expect that significant improvement of system performance as well as capacity is possible.

To analyze the performance of SBM/OFDM, the average bit-error rate (BER) performance of our proposed system is found by Monte Carlo simulation in frequency-selective fading channels and compared to a conventional single carrier system with smart antennas.

This paper is organized as follows. In Section II, the system model of SBM/OFDM is introduced. Section III provides analytical expressions for optimal antenna weights of SBM in a multicarrier system. Section IV considers the issues of multiple-access and proposes an iterative algorithm for ensuring the stability of the network and power optimization. Comparative simulation results are presented in Section V, and finally, we have some concluding remarks in Section VI.

II. SBM/OFDM System Model

The modem configuration of SBM/OFDM is shown in Fig. 1. A serial-to-parallel buffer segments an N_f information bit sequence into N_c parallel output streams. In general, each stream can contain a different number of bits so that

$$N_f = \sum_{c=1}^{N_c} m_c. \tag{1}$$

A Life Cycle Assessment of the Mobile Communication System using UMTS

[1]SHANKAR KUMAR DAS,
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]PRATAP PRADHAN,
Barunei Institute of Engineering and Technology, Khordha, Odisha, India

Goal, scope, and context The purpose of this research is to assess the environmental sustainability of the UMTS mobile communication system in Switzerland using a Life Cycle Assessment (LCA). It is presented a baseline environmental impact profile for the UMTS (Universal Mobile Telecommunication System) and its predecessor, the GSM (Global System for Mobile Communication). The baseline assessment was a necessary first step in assessing the environmental impacts of mobile communication system use and growth, allowing for an assessment of its environmental sustainability.

Introduction

The demand for mobile communication services is globally on the rise. Mobile phone networks are being built rapidly and are mainly steered by economical and legislative drivers. Environmental aspects are mainly incorporated only for singular aspects like non-ionizing radiation of antennae and mobile phones, or the energy use of switching centers. A complete picture of the different environmental impacts of the UMTS (Universal Mobile Telecommunication System) allows operators and manufacturers to intensify actions concentrating on the components of the whole system with the highest potential of improving their environmental properties.

Several studies have assessed environmental aspects of telecommunication systems (e.g. Oiva 2000) for a mobile phone, (Harada 2001) for the fixed network in Japan, (Blazek 1999) for the telecommunication systems of two cities). A study of the complete UMTS network is being done for Ericsson components; first results were presented in (Malmodin 2001). The study presented in this article is the first environmental assessment of UMTS in Switzerland.

1 Goal and Scope

Goal of the project is to assess the environmental sustainability of the Swiss UMTS network, which is currently being built by different telecommunication operators in Switzerland (Faist Emmenegger et al. 2003a). In order to do this, a life cycle assessment was carried out. The goal of the LCA is to assess the environmental impacts caused by a call via the UMTS mobile phone system. The results of the life cycle assessment (LCA) are used to quantify the environmental impact of the use and growth of the total UMTS mobile phone system and its components, thus making an assessment of its environmental impacts possible. All the components of the UMTS like the mobile phones, base stations, antennae and switching systems, and the components of the landline like cable system and switching centers, are assessed. The environmental impacts are assessed taking into account all major life cycle phases like raw material extraction, manufacturing, use, disassembly and disposal of the product and the needed infrastructure. A baseline environmental impact profile across the full life cycle of the GSM (Global System for Mobile Communication) was also done and allows the comparison between the two networks.

1.1 Mobile networks

GSM, which was first introduced in 1991, is one of the leading digital cellular systems. Eight simultaneous calls can occupy the same radio frequency. It provides integrated voice mail, high-speed data, fax, paging and short message services capabilities, as well as secure communications. Originally a European standard for digital mobile telephony, GSM has become the world's most widely used mobile system in use in over 100 countries. GSM networks operate on the 900 MHz and 1800 MHz waveband in Europe, Asia and Australia, and on the 1900 MHz waveband in North America and in parts of Latin America and Africa.

UMTS is the name for the third generation mobile telephone standard in Europe. 3G is a generic term covering a range of future wireless network technologies, including UMTS, WCDMA (Wideband Code-Division Multiple-Access), CDMA (Code-Division Multiple-Access) 2000 and EDGE (Enhanced Data rates for GSM Evolution). 3G combines high-speed mobile access with Internet Protocol (IP) based services.

1.2 Functional unit

Functional Unit Data Transfer. As a functional unit, a data set of 1 Gbit (1,000,000 kbit) is defined. For most of the network components, the normalization of manufacturing, installation, operating and disposal expenditure per transferred data set is required. In the UMTS, both data packages and calls can be conveyed. In order to be able to standardize the results, an equivalence is formed between these two kinds of transmission. This is based on the assumption of an average transmission rate of data packages and calls as well as on assumptions for the average use of the UMTS equipment by the customer. Based on an average minute of use the time share of data transfer in 2004 was determined. The total kb per year were calculated on the basis of an average data throughput (kb/s), the anticipated number of users and utilization ratio of the data throughput. Data used are based on planning network data and anticipated number of users for 2004. It can be assumed that the calculated network has some over-capacity as the licence asks from the operators to secure a certain coverage independent of the actual demand.

As a basis for the GSM (Global System for Mobile Commu-

Scalable acceptance algorithm in Wireless Ad Hoc Networks

[1]SULOCHANA NANDA,

Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]HEMANTA KUMAR BARIK,

R K Institute of Engineering & Technology, Cuttack, Odisha, India

Abstract— *Nodes in wireless ad hoc networks communicate with distant destinations via intermediate nodes acting as relays. Because wireless nodes have limited energy, it may not be in a node's best interest to always accept relay requests. However, if all nodes decide not to spend energy on relaying, network throughput will plummet dramatically. Both of these extreme scenarios (complete cooperation and complete non-cooperation) are detrimental to a user's interests. In this paper, we look at user cooperation in ad hoc networks. We assume that nodes are rational, meaning that their actions are solely motivated by self-interest, and that each node is bound by a minimum lifetime constraint. Given these lifetime constraints and the underlying assumption of rational behaviour,*

Methods keywords – Economics (game theory), System Design.

I. Introduction

Wireless ad hoc networks have matured as a viable means to provide ubiquitous untethered communication. In order to enhance network connectivity, a source communicates with far off destinations by using intermediate nodes as relays [1], [2], [3], [4]. However, the limitation of finite energy supply raises concerns about the traditional belief that nodes in ad hoc networks will always relay packets for each other. Consider a user in a campus environment equipped with a laptop. As part of his daily activity, the user may participate in different ad hoc networks in classrooms, the library and coffee shops. He might expect that his battery-powered laptop will last without recharging until the end of the day. When he participates in these different ad hoc networks, he will be expected to relay traffic for other users. If he accepts all relay requests, he might run out of energy prematurely. Therefore, to extend his lifetime, he might decide to reject all relay requests. If every user argues in this fashion, then the throughput that each user receives will drop dramatically. We can see that there is a trade-off between an individual user's lifetime and throughput.

Cooperation among nodes in an ad hoc network has been previously addressed in [5], [6], [7], [8], [9]. In [5], nodes, which agree to relay traffic but do not, are termed as misbehaving. Clever means to identify misbehaving users and avoid routing through these nodes are proposed. Their approach consists of two applications: *Watchdog* and *Pathrater*. The former runs on every node keeping track of how the other nodes behave; the latter uses this information to calculate the route with the highest reliability. In [6], [7], [8], a secure mechanism to stimulate nodes to cooperate and to prevent them from overloading the network is presented. The key idea is that nodes providing a service should be remunerated, while nodes receiving a service should be charged. Based on this concept, an acceptance algorithm is proposed. The acceptance algorithm is used to decide whether to accept or reject a packet relay request. The acceptance algorithm at each node attempts to balance the number of packets it has relayed with the number of its packets that have been relayed by others. The drawback of this scheme is that it involves per packet processing which results in large overheads. In [9], two acceptance algorithms are proposed, which are used by the network nodes to decide whether to relay traffic on a per session basis. The goal of these algorithms is to balance the energy consumed by a node in relaying traffic for others with energy consumed by other nodes in relaying traffic and to find an optimal trade-off between energy consumption and session blocking probability. By taking decisions on a per session basis, the per packet processing overhead of previous schemes is eliminated. We emphasize, however, that all the above algorithms are based on heuristics and lack a formal framework to analyze the optimal trade-off between lifetime and throughput.

In this paper, we consider a finite population of N nodes (e.g., students on a campus). Each node, depending on its type (e.g., laptop, PDA, cell phone), is associated with an average power constraint. This constraint can be derived by dividing its initial energy allocation by its lifetime expectation. We assume that time is slotted and that each session lasts for one slot. We deal with connection-oriented traffic. At the beginning of each slot, a source, destination and several relays are randomly chosen out of the N nodes to form an ad hoc network (e.g., students in a coffee shop). The source requests the relay nodes in the route to forward its traffic to the destination. If any of the relay nodes rejects the request, the traffic connection is blocked.

For each node, we define the *Normalized Acceptance Rate* (NAR) as the ratio of the number of successful relay requests generated by the node, to the number of relay requests made

Mobile Ad-hoc Networks (MANET): A Review

[1]SUPRIYA JENA,
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]MANORANJAN AICH,
Barunei Institute of Engineering and Technology, Khordha, Odisha, India

Abstract

Mobile Ad-hoc networks, which were first deployed in the 1990s, have been the subject of extensive research for many years. Mobile Ad-hoc Networks are made up of two or more devices that have wireless communications and networking capabilities. These devices can communicate with nodes that are either within their radio range or outside their radio range. In the latter case, the nodes should deploy an intermediate node to act as a router, routing packets from the source to the destination. Because Wireless Ad-hoc Networks lack a gateway, any node can act as the gateway. Although much research has been done in this field since the 1990s, it has frequently been questioned whether the architecture of Mobile Ad-hoc Networks is fundamentally flawed.

We take the position that Mobile Ad-hoc Networks (MANET) are a fundamentally flawed architecture. As argument, we try to clarify the definition, architecture and the characters of MANET, as well as the main challenges of constructing the MANET. Although many works have been done to solve the problem, we will show in this paper that it is very difficult to solve these limitations which made the Mobile Ad-hoc Networks a flawed architecture.

After giving many evidences and analysis, we could see that the key technologies of Wireless Ad-hoc Networks were not implemented as well as we expect. That is to say, many problems are inherently unsolvable. Thus, we could explain why we take the position that Mobile Ad-hoc Networks are flawed architecture.

1. Introduction

Research on Wireless Ad Hoc Networks has been ongoing for decades. The history of wireless ad hoc networks can be traced back to the Defense Advanced Research Project Agency (DAPRPA) packet radio networks (PRNet), which evolved into the survivable adaptive radio networks (SURAD) program [11]. Ad hoc networks have play an important role in military applications and related research efforts, for example, the global mobile information systems (GloMo) program [12] and the near-term digital radio (NTDR) program [13]. Recent years have seen a new spate of industrial and commercial applications for wireless ad hoc networks, as viable communication equipment and portable computers become more compact and available.

Since their emergence in 1970's, wireless networks have become increasingly popular in the communication industry. These networks provide mobile users with ubiquitous computing capability and information access regardless of the users' location. There are currently two variations of mobile wireless networks: infrastructured and infrastructureless networks.

The infrastructured networks have fixed and wired gateways or the fixed Base-Stations which are connected to other Base-Stations through wires. Each node is within the range of a Base-Station. A "Hand-off" occurs as mobile host travels out of range of one Base-Station and into the range of another and thus, mobile host is able to continue communication seamlessly throughout the network. Example applications of this type include wireless local area networks and Mobile Phone.

The other type of wireless network, ***infrastructureless networks***, is knows as **Mobile Ad-hoc Networks (MANET).** These networks have no fixed routers, every node could be router. All nodes are capable of movement and can be connected dynamically in arbitrary manner. The responsibilities for organizing and controlling the

Performance analysis of Routing Security in Wireless Ad Hoc Networks

[1]TAPAN KUMAR PRADHAN,
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]RAMESH CHANDRA SETHY,
R K Institute of Engineering & Technology, Cuttack, Odisha, India

ABSTRACT

A mobile ad hoc network is made up of wireless mobile nodes that can communicate with one another without the use of a network infrastructure or centralised administration. MANET is a new research area with real-world applications. However, due to fundamental characteristics such as open medium, dynamic topology, distributed cooperation, and constrained capability, wireless MANET is particularly vulnerable. Routing is critical to the overall security of the network. In general, routing security in wireless MANETs appears to be a difficult problem to solve. In this article, we examine the routing security issues of MANETs and examine in detail one type of attack — the "black hole" problem — that can be easily used.

There has been explosive growth in the use of wireless communications over the last few years, from satellite transmission to home wireless personal area networks. The primary advantage of a wireless network is the ability of the wireless node to communicate with the rest of the world while being mobile. Two basic system models have been developed for the wireless network paradigm. The fixed backbone wireless system model consists of a large number of mobile nodes and relatively fewer, but more powerful, fixed nodes. These fixed nodes are hard wired using landlines. The communication between a fixed node and a mobile node within its range occurs via the wireless medium. However, this requires a fixed permanent infrastructure. Another system model, the *mobile ad hoc network* (MANET) has been proposed to set up a network when needed; however, the transmission range of each low-power node is limited to each other's proximity, and out-of-range nodes are routed through intermediate nodes.

A MANET is considered a collection of wireless mobile nodes that are capable of communicating with each other without the use of a network infrastructure or any centralized administration. The mobile hosts are not bound to any centralized control like base stations or mobile switching centers. Although this offers unrestricted mobility and connectivity to the users, the onus of network management is now entirely on the nodes that form the network. Due to the limited transmission range of wireless network interfaces, multiple hops may be needed for one node to exchange data with another across the network. In such a network, each mobile node operates not only as a host but also as a router, forwarding packets for other mobile nodes in the network that may not be within direct wireless transmission range of each other. Each node participates in an ad hoc routing protocol that allows it to discover multihop paths through the network to any other node. The idea of MANET is also called *infrastructureless networking*, since the mobile nodes in the network dynamically establish routing among themselves to form their own network on the fly. It is formed instantaneously, and uses multihop routing to transmit information. MANET technology can provide an extremely flexible method of establishing communications in situations where geographical or terrestrial constraints demand a totally distributed network system without any fixed base station, such as battlefields, military applications, and other emergency and disaster situations. A sensor network, which consists of several thousand small low-powered nodes with sensing capabilities, is one of the futuristic applications of MANET. Figure 1 shows example applications of wireless MANETs. Obviously, security is a critical issue in such areas.

However, recent wireless research indicates that the wireless MANET presents a larger security problem than conventional wired and wireless networks [1, 2]. While most of the underlying features make MANETs useful and popular.

First, all signals go through bandwidth-constrained wireless links in a MANET, which

Design analysis of Simulation Tools for Wireless Sensor Networks (WSNs)

[1]AJANTA PRIYADARSHINI,
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]SANTANU KUMAR PATRA,
SakuntalaSudarsan Institute of Technology, Mayurbhanj, Odisha, India

Abstract *The adoption of Wireless Sensor Networks has increased in recent years due to their diverse applications in a variety of fields. A wireless sensor network is created by connecting a large number of sensor nodes. Each sensor node in the network monitors various parameters such as temperature, humidity, ambient light, gas, and so on and sends the data to the master node. Despite their numerous applications and diverse uses, sensor networks suffer from a variety of shortcomings such as energy, localization, security, self-organization, fault tolerance, and many others. As a result, various researchers around the world are conducting rigorous research and development to develop new algorithms, protocols, and techniques to make WSN networks more efficient and reliable. Testing of the developed technique is required prior to live implementation.*

Keywords Wireless Sensor Networks, Simulation Tools, Comparison, Performance Evaluation, Network Simulator

1. Introduction

In recent years, tons of new and advanced research has been done and is also picking up in the area of Wireless Sensor Networks [1] and this area is also catching the viral attention of researchers from all parts of the world for developing wide applications and making use of WSN networks in varied fields. Wireless Sensor Network comprises of a large number of sensor nodes having sensing and computing capabilities and are deployed in random manner. Each of the sensing devices in WSN network is called MOTE [2].

The following figure shows a view of simple wireless sensor network. Wireless sensor network [4] consists of one or more base stations known as gateways, a number of sensor nodes and end user. The output generated by one node is wirelessly transmitted to the base station for data collection, analysis and logging. Each and every node in the Wireless Sensor Network acts as router for transmitting the information from source node to sink node [122] [123] [125]. The end users are facilitated with the data from the sensor via some website or some application in the console terminal.

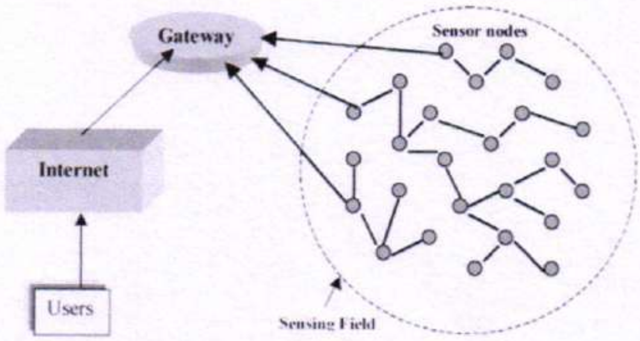


Figure 1. Simple Wireless Sensor Network

Sensor Networks face various kinds of issues which normally don't occur in other sorts of networks [1-4] like power constraints, resource constraints, hardware availability, low communication range, limited processing and storage, cost etc.

As the cost, time and complexity involved in the deployment as well as implementation in such networks is very high, so developers preferably like to get first-hand information on feasibility and reflectivity which is very important for implementation of system before hardware

A Security threat analysis of Wireless Sensor Networks Applications

[1]ANKITA MUHURI,
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]SURESH CHANDRA SAHOO,
Barunei Institute of Engineering and Technology, Khordha, Odisha, India

Abstract— *Wireless communication technologies continue to advance at a rapid pace. In recent years, there has been a significant increase in research in the field of wireless sensor networks (WSNs). WSNs communicate using spatially distributed, autonomous sensor nodes that are equipped to sense specific information. WSNs are used in a wide range of military and civilian applications around the world. Detecting enemy intrusion on the battlefield, object tracking, habitat monitoring, patient monitoring, and fire detection are some examples. Sensor networks are emerging as an appealing technology with great future potential. However, issues concerning coverage and deployment, scalability, quality-of-service, size, computational power, energy efficiency, and security must still be addressed. This paper provides an overview of the various wireless applications.*

Index Terms—**Network, Security, Sensor, Wireless.**

I. INTRODUCTION

A wireless sensor network (WSN) [1] [2] is a wireless network consisting of spatially distributed autonomous devices that use sensors to monitor physical or environmental conditions. These autonomous devices, or nodes, combine with routers and a gateway to create a typical WSN system. The distributed measurement nodes communicate wirelessly to a central gateway, which provides a connection to the wired world where you can collect, process, analyze, and present your measurement data. To extend distance and reliability in a wireless sensor network, you can use routers to gain an additional communication link between end nodes and the gateway. Currently, wireless sensor networks are beginning to be deployed at an accelerated pace. It is not unreasonable to expect that in 10-15 years that the world will be covered with wireless sensor networks with access to them via the Internet (Figure-1). This can be considered as the Internet becoming a physical network. This new technology is exciting with unlimited potential for numerous application areas including environmental, medical, military, transportation, entertainment, crisis management, homeland defense, and smart spaces.

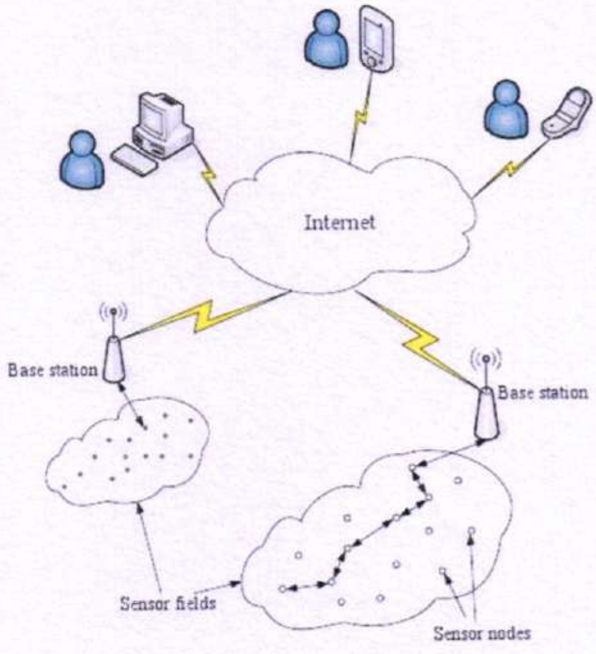


Figure-1 Accessing WSNs through Internet.

The major challenges to be addressed in WSNs are coverage and deployment, scalability, quality- of- service, size, computational power, energy efficiency and security[3]. Among these challenges, security is a major issue in wireless sensor networks. Most of the threats and attacks against security in wireless networks are almost similar to their wired counterparts while some are exacerbated with the inclusion of wireless connectivity. In fact, wireless networks are usually more vulnerable to various security threats as the unguided transmission medium is more susceptible to security attacks than those of the guided transmission medium. The broadcast nature of the wireless communication is a simple candidate for eavesdropping. In this paper we present an overview of the applications and security issues relating to Wireless Sensor Networks(WSNs).

II. APPLICATIONS OF WIRELESS SENSOR NETWORKS

A. Military or Border Surveillance Applications

WSNs are becoming an integral part of military command, control, communication and intelligence systems. Sensors can be deployed in a battle field to monitor the presence of forces and vehicles, and track their movements, enabling close surveillance of opposing forces.

Monitoring Wireless Sensor Networks in the Railway Industry: A Survey

[1]BIJOY TAPAN MOHAN NAYAK,
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]KAILASH CHANDRA SAHOO,
Barunei Institute of Engineering and Technology, Khordha, Odisha, India

***Abstract*— *Sensor technology has rapidly expanded in recent years, while sensor devices have become more affordable. This has resulted in a rapid increase in the use of sensors to monitor the condition of systems, structures, vehicles, and machinery. Recent advancements in networking technologies such as wireless communication and mobile ad hoc networking, as well as device integration technology, are critical factors. WSNs can be used to monitor railway infrastructure such as bridges, rail tracks, track beds, and track equipment, as well as vehicle health such as chassis, bogies, wheels, and waggons. Condition monitoring reduces the need for human inspections through automated monitoring, lowers maintenance costs by detecting faults before they escalate, and improves safety and reliability. This is critical for growth, improvement, and expansion.*

***Index Terms*—Asset management, condition monitoring, decision support systems, event detection, maintenance engineering, preventive maintenance, railway engineering, wireless sensor networks (WSNs).**

I. Introduction

EXPERTS estimate that the railway industry will receive US$300 billion worth of global investment for development, upgrading, and expansion over the five years from 2009 [43]. Ollier [98] noted that effective management of rail infrastructure will be vital to this development, upgrading, and expansion, particularly if coupled with a move to intelligent infrastructure [39]. A key part of the management will be condition monitoring. Condition monitoring detects and identifies deterioration in structures and infrastructure before the deterioration causes a failure or prevents rail operations. In simple condition monitoring, sensors monitor the condition of a structure or machinery. If the sensor readings reach a predetermined limit or fault condition, then an alarm is activated. However, this simplistic approach may lead to a large number of false alarms and missed failures [36]. It only provides local analysis but does not take advantage of the superior capabilities when the sensors are networked and their data processed collectively. Integrated data processing allows an overall picture of an asset's condition to be achieved and overall condition trends to be determined [97].

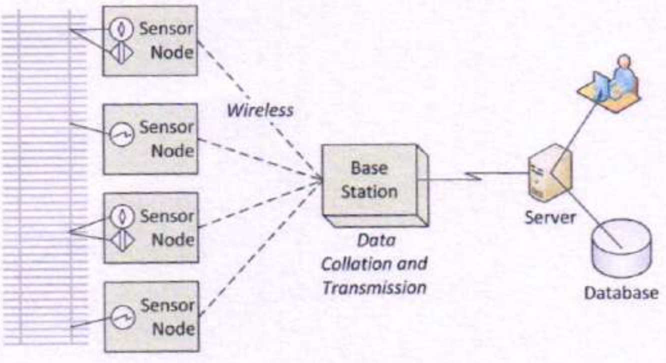


Fig. 1. Figure shows a typical WSN setup for railway condition monitoring. Sensor devices are mounted on boards attached to the object being monitored; examples include track, bridges, or train mechanics. One or more sensors are mounted on a sensor board (node) (see also Fig. 2). The sensor nodes communicate with the base station using a wireless transmission protocol; examples include Bluetooth and Wi-Fi. The base station collates data and transmits it to the control center server possibly through satellite or GPRS. There are variations on this setup. In some systems, the sensor nodes may communicate directly with the server rather than via the base station. In other systems, the user accesses the data directly via the base station.

In recent years, networking technologies such as wireless communication and mobile *ad hoc* networking coupled with the technology to integrate devices have rapidly developed. The new technologies allow vast numbers of distributed sensors to be networked [5], [6], [37], [45], [122] to constantly monitor machines, systems, and environments. Wireless sensor networks (WSNs) [5], [134] are wireless networks of spatially distributed and autonomous devices. They use sensors to cooperatively monitor infrastructure, structures, and machinery. A typical WSN for railway applications is shown in Fig. 1. Each sensor node generally has a radio transceiver, a small microcontroller, and an energy source, usually a battery (see Section II-C for more detail). WSNs and data analytics allow the railways to turn data into intelligence [43]. They provide decision support through continuous real-time data capture and analysis to identify faults [52]. The data from distributed systems such as sensor networks are constantly monitored using classification [56], [57], prediction [85], or anomaly detection [61] to determine the current and future status of the distributed network. Lopez-Higuera *et al.* [78] developed a staircase of

A deterministic deployment strategy for Wireless Sensor Networks (WSNs) Deployment

[1]GYANENDRA KUMAR ROUT,
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]SUBASH CHANDRA SAHOO,
SakuntalaSudarsan Institute of Technology, Mayurbhanj, Odisha, India

Abstract *– Device deployment is a critical aspect of WSN provisioning. Many intrinsic properties of a WSN, such as coverage, connectivity, cost, and lifetime, are determined by the types, number, and location of devices. In this paper, we investigate the problem of optimal WSN deployment with the goal of minimising network cost under lifetime constraints. We talk about and identify the characteristics of a specific type of WSN application. The end goals of device deployment for such applications are presented and discussed. In a practical and fundamental scenario, we refine a deployment problem. The minimum set covering problem is used to model this problem. A deterministic deployment strategy is proposed based on a recursive algorithm.*

Keywords: **Wireless Sensor Networks, Cost, Lifetime, Coverage, Connectivity, Deployment, Minimum Set Covering**

I. INTRODUCTION

A WSN has two major functions, i.e., sensing and communication. That is, the sensors sense (proactively or reactively) the environment and report the data to the end-user. Coverage and connectivity are the factors that determine the efficacy of sensing and communication, respectively.

A sensing field is considered to be completely **covered** if every point in the field (regular or irregular area) is within the sensing range of an active sensor in a desired degree. The demanded coverage is ensured by a deployment strategy, which determines where to place what type of sensor node (in case of heterogeneous network, nodes are different by sensing capability, communication capability, power capacity, etc). A WSN is considered to be fully **connected** if all nodes can deliver their data to the destination, such as a Base Station (BS) [Sch03]. Deployment and communication mechanisms are two critical techniques to jointly provide connectivity.

Other major concerns of a WSN, from a user's point of view, are cost and lifetime. They are of the essential criteria to evaluate a WSN or choose a WSN design from a number of candidates. It is desirable to have a WSN function for a guaranteed lifespan at a minimum cost, or operate as long as possible under a certain cost budget. Generally, reducing the device cost and prolonging the network lifetime may be contradictory to each other. For example, lifetime can be extended by upgrading the battery capacity of devices or increasing the number of nodes. Either of the two methods leads to an increase of device cost. A well designed deployment strategy and appropriate communication mechanism can achieve a desired tradeoff between the two factors.

This paper aims at the deployment strategy of a type of WSNs in civilian applications, such as, building automation, residential control, commercial control, industrial control, and etc. For example, a WSN can foster a smart space which is "watched" by various inter-connected sensors to provide building automation. The various physical quantities measured and reported by the sensor nodes will enable an efficient management of lighting, heating, ventilating, air conditioning, surveillance, etc. From this example, the major features of typical civilian applications can be summarized as follows:

1) **Pre-fixed or traceable sensing spots**. The sensing spots are application determined and known a priori when planning a WSN. In such a case, the location and the number of sensor nodes are determined. For instance, motion control sensors can be deployed at the entrance of a room so that the light can be turned on automatically when people walk in; temperature sensors can be placed in each room so that the heating and cooling can be automatically adjusted for each room at individual preferences.

2) **Co-existence of heterogeneous devices**. A civilian WSN usually consists of a large number of small size devices. Each device will take different duties, such as sensing different physical quantitative, routing and relaying, data processing and aggregating, clustering and coordinating. On the other hand, manufacturers of different expertise can provide products with different functions at different price. For example, of the 70 members in ZigBee Alliance nowadays, Honeywell and Omron specialize in sensing and control, while Motorola and Samsung are famous for their networking technology [Zigbee]. These products may also be different in power supply, computation ability, communication range, etc.

We consider constructing a WSN by utilizing the diversified devices. Based on the characteristics of the WSN applications presented above, we assume the sensing spots are known in advance. The heterogeneity of devices raises a challenge on how to sufficiently and fairly utilize the resources of different devices, so that the network lifetime is extended.

Challenges in Wireless Sensor Networks

[1]HIMANSHU SEKHAR MOHARANA,
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]HIRENDRANATH SWAIN,
PadmashreeKrutarthaAcharya Institute of Engineering & Technology, Baragarh, Odiaha, India

Abstract — *Wireless Sensor Network (WSN) is a new technology that holds great promise for a variety of future applications, both civilian and military. The combination of sensing technology, processing power, and wireless communication makes it lucrative for future use. The use of wireless communication technology also introduces new security risks. The purpose of this paper is to look into security issues and challenges in wireless sensor networks. We examine proposed security mechanisms for wireless sensor networks and identify security threats. We also talk about how to take a holistic approach to security to ensure layered and robust security in wireless sensor networks. WSN provisioning is fundamentally concerned with deployment. Many intrinsic properties of a system are determined by the types, number, and locations of devices.*

Keywords — **Sensor, Security, Attack, Holistic, Challenge.**

1. Introduction

Wireless Sensor Networks (WSN) are emerging as both an important new tier in the IT ecosystem and a rich domain of active research involving hardware and system design, networking, distributed algorithms, programming models, data management, security and social factors [1], [2], [3]. The basic idea of sensor network is to disperse tiny sensing devices; which are capable of sensing some changes of incidents/parameters and communicating with other devices, over a specific geographic area for some specific purposes like target tracking, surveillance, environmental monitoring etc. Today's sensors can monitor temperature, pressure, humidity, soil makeup, vehicular movement, noise levels, lighting conditions, the presence or absence of certain kinds of objects or substances, mechanical stress levels on attached objects, and other properties [4]. In case of wireless sensor network, the communication among the sensors is done using wireless transceivers. The attractive features of the wireless sensor networks attracted many researchers to work on various issues related to these types of networks. However, while the routing strategies and wireless sensor network modeling are getting much preference, the security issues are yet to receive extensive focus. In this paper, we explore the security issues and challenges for next generation wireless sensor networks and discuss the crucial parameters that require extensive investigations.

Basically the major challenge for employing any efficient security scheme in wireless sensor networks is created by the size of sensors, consequently the processing power, memory and type of tasks expected from the sensors. We discuss these issues and challenges in this paper. To address the critical security issues in wireless sensor networks we talk about cryptography, steganography and other basics of network security and their applicability in Section 2. We explore various types of threats and attacks against wireless sensor network in Section 3. Section 4 reviews the related works and proposed schemes concerning security in WSN and also introduces the view of holistic security in WSN. Finally Section 5 concludes the paper delineating the research challenges and future trends toward the research in wireless sensor network security.

2. Feasibility of Basic Security Schemes in Wireless Sensor Networks

Security is a broadly used term encompassing the characteristics of authentication, integrity, privacy, nonrepudiation, and anti-playback [5]. The more the dependency on the information provided by the networks has been increased, the more the risk of secure transmission of information over the networks has increased. For the secure transmission of various types of information over networks, several cryptographic, steganographic and other techniques are used which are well known. In this section, we discuss the network security fundamentals and how the techniques are meant for wireless sensor networks.

2.1 Cryptography

The encryption-decryption techniques devised for the traditional wired networks are not feasible to be applied directly for the wireless networks and in particular for wireless sensor networks. WSNs consist of tiny sensors which really suffer from the lack of processing, memory and battery power [6], [7], [8], [9]. Applying any encryption scheme requires transmission of extra bits, hence extra processing, memory and battery power which are very important resources for the sensors' longevity. Applying the security mechanisms such as encryption could also increase delay, jitter and packet loss in wireless sensor networks [10]. Moreover, some critical questions arise when applying encryption schemes to WSNs like, how the keys are generated or disseminated. How the keys are managed, revoked, assigned to a new sensor added to the network or renewed for ensuring robust security for the

An Overview of defence related applications of wireless sensor networks (WSNs)

[1]MANORAMA SUBUDHI,
Gandhi Institute of Excellent Technocrats,
Bhubaneswar, India

[2]AKSHAYA KUMAR BATA,
Aumsai Institute of Technical Education,
Berhampur, Odisha, India

Abstract— This paper provides an overview of wireless sensor network applications in defence (WSNs). The operational context of modern military engagement has evolved into four scenarios, each with its own set of requirements and constraints for WSN applications. The types of sensors and their capabilities determine and limit the application of WSNs. We categorise military WSN applications based on operation scenarios and sensor types, and we describe key classes. We also talk about future generations of military WSN applications in terms of research and engineering.

Keywords-wireless sensor networks; battlefield; urban; other-than-war; force protection; presence; CBRNE; ranging; imaging

I. INTRODUCTION

Communications is present in almost all aspects of military operations [1]. It is important in the distribution of commands and ensures distribution of logistical information, intelligence and data from sensors. In this work, we survey military applications based on collecting data from sensors by use of wireless sensor networks (WSNs).

Military communications, by any means, must be maintained in the area and time where needed [1]. In general, they should be resistant to jamming, direction finding and other electronic warfare threats, and provide end-to-end message security. This also holds for military WSN communications.

In a common battlefield scenario of military engagement there is a well-known and well-defined enemy, in the air, on land or at sea. However, recent experience has revealed more scenarios, such as truly worldwide operations, operations in urban environment, and operations other than war (OTW) e.g. peacekeeping and disaster relief [1]. We consider applications of WSNs in a large area battlefield (but not worldwide), urban warfare, OTW and force protection. The latter intersects with the first three scenarios. Its requirements are discussed in [2].

The capabilities of military WSN applications depend not only on wireless communications fulfilling the requirements mentioned above, but also on the capabilities of sensors. The sensors measure various physical phenomena. Some of the most important in military applications are electromagnetic waves, light, pressure and sound, which result from gunfire and explosions. Sensors can detect and possibly measure chemical, biological and explosive vapor, as well as presence of people or objects. We will use the sensor capabilities as one of key determinants of the type of military application of WSNs.

Irrespective of the scenario and the sensor type, the WSNs are mostly useful in providing a cost-effective method of gathering information about the environment, and actors in that environment [1]. In the cases of battlefield, urban warfare and force protection, the use of WSNs can reduce the uncertainty over where the enemy forces will be deployed or what role they will be fulfilling. In OTW scenarios, the use of WSNs can reduce uncertainty over where the population which needs to be protected is, and which areas are at risk of natural disaster.

The data measured by sensors is sent from the sensor nodes to one or more gateways, after possible pre-processing. The gateways can provide data fusion, additional data processing, and the reach-back capability [2]: near real time connection via longer range wireless transmissions or satellite links; and asynchronous data transfer to passing unmanned aerial vehicles.

A tiered WSN architecture for military surveillance applications is proposed in [3]. The hierarchical architecture is built using sensor nodes with short-range radio and wireless gateways with wireless long-haul connectivity. This architecture affords greater agility and expandability, with possible operations from a small-scale single cluster of sensor nodes to many chained connections spanning a large area [3].

The communication architectures influence the coverage and connectivity of WSNs, which in turn set the performance and limitations of military applications of WSNs. A survey of coverage in WSNs and related issues is provided in [4].

The rest of the paper is structured as follows. Section II. presents a classification of military applications of WSNs. Section III. describes the main classes identified in Section II. Section IV. presents a discussion of research and engineering challenges in military applications of WSNs. Section V. concludes the paper.

An optimistic approach for resolving the issues in Wireless Sensor Networks

[1]MRUTYUNJAYA SENAPATI,
*Gandhi Institute of Excellent Technocrats,
Bhubaneswar, India*

[2]BHARAT DEWANGAN,
*Sanjay Memorial Institute
of Technology, Ganjam,
Odisha, India*

Abstract— *Recent technological advancements have encouraged researchers to be optimistic about the viability of wireless sensor networks (WSNs). These are being used for a variety of applications and have enormous research potential. However, due to the multidisciplinary nature of this field, researchers face numerous technical challenges. This paper provides an overview of the broad research issues and challenges involved in the design of WSNs. Energy conservation emerges as one of the most critical aspects in hardware and software design issues, casting doubt on the overall viability of WSNs. Other major issues include specialised hardware, software, and operating systems, synchronisation, QoS, security, architecture, and data collection with low communication and computation costs.*

Keywords- WSN, issues, challenges, security, QoS, management

I. INTRODUCTION

In recent years, development and deployment of wireless sensor networks (WSNs) is growing on rapid pace. Wireless Sensor Network [1,2] consists of large number of sensor nodes (small and cost effective sensing devices with wireless radio transceiver) over a wide area mainly to monitor the environment that does not have infrastructure like power supply, wired internet connection and without human interaction. Each sensor node, having one or more sensors, is capable to collect, compute and communicate to other nodes. Sensor nodes are capable of sensing physical parameters like temperature, humidity, chemical composition etc. from the sensing field. The sensed data is then processed at node level or cluster level and communicated to sink or base station generally referred as collection points. Rapid deployment, self organization, high sensing fidelity, flexibility, low cost and fault tolerance characteristics of WSNs make them a very promising sensing technique for various applications. WSNs are very useful to collect information from those areas where it is difficult to reach and are seldom accessible. Promising applications of WSN include wide area monitoring for personnel/ vehicles, secure area intrusion monitoring and denial, environmental monitoring, animal habitats, migration, forest fires, natural disasters, subsea monitoring, building monitoring, vehicle traffic monitoring and control, remote site power substation monitoring, patient monitoring, smart home and inventory management and many other real life applications [3,4] for sensor deployments.

Wireless sense and control technology is being utilized to bridge the gap between the physical world of humans and the virtual world of electronics. WSNs hold the potential to provide low cost solution for the problems in military, medical and climatic conditions. The dream is to automatically monitor and respond to forest fires, avalanches, hurricanes, faults in countrywide utility equipments, traffic, hospitals and much more wide areas and with billions of sensors. However, owing to limited storage capacity and power of sensor nodes, numerous research issues and challenges are being faced by researchers while setting up a workable sensor network. This research paper presents an exploratory summary of these challenges and constraints for the overall benefit of researchers working in this challenging area in the following section.

II. RESEARCH ISSUES AND CHALLENGES IN WSNs

Major issues that affect the design and performance of a wireless sensor network are as follows:

- **Energy:** Sensors require power for various operations. Energy [5,6] is consumed in data collection, data processing, and data communication; also, continuous listening to the medium for faithful operation demands a large amount of energy by node components (CPU, radio, etc.) even if they are idle. Batteries providing power need to be changed or recharged after they have been consumed. Sometimes it becomes difficult to recharge or change the batteries because of demographic conditions. The most crucial research challenge for the WSN researchers is to design, develop and implement energy efficient hardware and software protocols for WSNs.

- **Self Management:** Wireless sensor networks once deployed should be able to work without any human intervention. It should be able to manage the network configuration, adaptation, maintenance, and repair by itself [7,8].

- **Hardware and Software Issues:** Sensor Networks consists of hundreds of thousands of nodes. It is preferred only if the node is cheap. Flash memory is advised to be used in sensor networks as it is

Monitoring through Wireless Sensor Networks – A Survey

[1]NEHA SHARMA,
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]GAURAB RANJAN PAIKARAY,
PadmashreeKrutarthaAcharya Institute of Engineering & Technology, Baragarh, Odiaha, India

Abstract- *WSNs are spatially dispersed independent sensors that track physical objects or monitor environmental data and collectively transmit the data to a master station. WSN is used in a variety of applications, including animal tracking, precision agriculture, environmental monitoring, security and surveillance, smart buildings, and health care. This paper presents various WSN applications with the goal of disseminating various WSN applications for the research community's better understanding of WSN applications in further innovative fields.*

.INTRODUCTION

WSNs are built of nodes which consist of a radio transceiver, microcontroller and sensors. Sensors having different applications can be used so that it can perform well in any area. Mainly sensors are classified according to the readiness for field deployment that focuses in the field deployment in terms of economy and engineering efficiency, scalability and cost. The main categories of sensors are given as physical, chemical and biological sensors. The Wireless Sensor Networks consist of data acquisition network and data distribution network. The network will be managed and controlled by a central station. The data acquisition network in the wireless sensor network is used to acquire data from different fields. The acquired data is transmitted to the master station by means of different wireless distribution techniques. The wireless distribution techniques include transmission using cellular phones, Computers, WLAN, WI – Fi etc. Once the acquired data reaches the master station, the data is analyzed and further processing is done. The main characteristics of WSN includes: energy harvesting, ability to cope with node failure, mobility of nodes, heterogeneity of nodes, scalability to large scale deployment, ability to withstand harsh environmental conditions and ease of use. The mentioned features ensure a wide range of application of sensor networks. The main application areas of a wireless sensor network can be classified as shown in Fig 1 and its objectives are given in table 1.

I. WSN APPLICATIONS

A) Precision Agriculture

Precision agriculture aims at building cultural operations more resourceful, while reducing environmental impact. The information collected from sensors is used to appraise most favorable sowing density, estimate fertilizers and other inputs needs, and to more precisely predict crop yields. WSN plays

Integrating Constrained Application Protocol (CoAP) with Wireless Sensor Networks

[1]NIHARIKA SAHU,
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]VIMA LENKA,
PNS School Of Engineering & Technology, Kendrapara, Odisha, India

ABSTRACT

IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN) has accelerated the Internet integration of Wireless Sensor Networks (WSNs) and smart objects. Simultaneously, the Constrained Application Protocol (CoAP) has enabled the provision of RESTful web service functionality to resource-constrained devices, allowing WSNs and smart objects to be integrated with the Web. The use of Web services on top of IP-based WSNs improves software reusability and reduces application development complexity. RESTful WSNs are the focus of this work. It describes CoAP, highlights the main differences with HTTP, and reports the results of a simple experiment demonstrating the advantages of CoAP over HTTP in terms of power consumption. The paper also discusses the design and development processes.

Keywords

Web applications, Web of Things, REST, CoAP.

1. INTRODUCTION

Recent advances in Wireless Sensor Network (WSN) technology and the use of the Internet Protocol (IP) in resource constrained devices has radically changed the Internet landscape. Trillions of smart objects will be connected to the Internet to form the so called Internet of Things (IoT). The IoT will connect physical (analogic) environments to the (digital) Internet, unleashing exciting possibilities and challenges for a variety of application domains, such as smart metering, e-health logistics, building and home automation [7].

The use of IP technology on embedded devices has been recently promoted by the work of the IP for Smart Objects (IPSO) Alliance[1], a cluster of major IT/telecom players and wireless silicon vendors. At the same time, the Internet Engineering Task Force (IETF) has done substantial standardization activity on IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) [8]. This new standard enables the use of IPv6 in Low-power and Lossy Networks (LLNs), such as those based on the IEEE 802.15.4 standard [10]. In addition to 6LowPAN, IETF Routing over Low-power and Lossy networks (ROLL) Working Group has designed and specified a new IP routing protocol for smart object internetworking. The protocol is called IPv6 Routing Protocol for Low-power and Lossy networks (RPL) [9].

One of the major benefits of IP based networking in LLNs is to enable the use of standard web service architectures without using application gateways. As a consequence, smart objects will not only be integrated with the internet but also with the Web. This integration is defined as the Web of Things (WoT). The advantage of the WoT is that smart object applications can be built on top Representational State Transfer (REST) architectures. REST architectures allow applications to rely on loosely coupled services which can be shared and reused. In a REST architecture a resource is an abstraction controlled by the server and identified by a Universal Resource Identifier (URI). The resources are decoupled by the services and therefore resources can be arbitrarily represented by means of various formats, such as XML or JSON. The resources are accessed and manipulated by an application protocol based on client/server request/responses. REST is not tied to a particular application protocol. However, the vast majority of REST architectures nowadays use Hypertext Transfer Protocol (HTTP). HTTP manipulates resources by means of its methods *GET*, *POST*, *PUT*, etc [6].

REST architectures allow IoT and Machine-to-Machine (M2M) applications to be developed on top of web services which can be shared and reused. The sensors become abstract resources identified by URIs, represented with arbitrary formats and manipulated with the same methods as HTTP. As a consequence, RESTful WSNs drastically reduce the application development complexity.

The use of web service in LLNs is not straightforward as a consequence of the differences between Internet applications and IoT or M2M applications. IoT or M2M applications are short-lived and web services reside in battery operated devices which most of the time sleep and wakeup only when there is data traffic to be exchanged. In addition, such applications require a multicast and asynchronous communication compared to the unicast and synchronous approach of standard Internet applications [11].

The Internet Engineering Task Force (IETF) Constrained RESTful environments (CoRE) Working Group has done major standardization work for introducing the web service paradigm into networks of smart objects. The CoRE group has defined a REST based web transfer protocol called Constrained Application Protocol (CoAP). CoAP includes the HTTP functionalities which have been re-designed taking into account the low processing power and energy consumption constraints of small embedded

MEMS-accelerometer based monitoring in end-milling using wireless sensor networks (WSNs)

[1]NITESH KUMAR MAHATO,

Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]BHIKARI CHARAN SETHI,

PadmashreeKrutarthaAcharya Institute of Engineering & Technology, Baragarh, Odiaha, India

KEYWORDS

Wireless Sensors, Machine Monitoring, MEMS-Accelerometers, Surface Finish

ABSTRACT

The purpose of this paper is to discuss the overall potential of wireless sensor nodes and networking in manufacturing environments. A specific case study that developed the enabling infrastructure for MEMS-accelerometer-based monitoring of machine tool vibrations is described. The case study's focus was not on vibration analysis per se. Experiments were conducted instead to demonstrate that wireless sensor networks, and their individual wireless sensor platforms, could provide new tools for research in predictive maintenance and condition-based monitoring of factory machinery in general, and for "open architecture machining systems" in particular. The case study tests revealed a linear relationship between surface finish, tool wear, and machine tool vibrations. Thus, a MEMS-accelerometer-based WSN platform supported by the WSN was demonstrated.

INTRODUCTION

Wireless sensor networks (WSNs) are *ad hoc* local area networks (LANs) created from small, inter-connected wireless platforms. Each platform carries sensors suitable for the desired industrial, residential, or civil application. Often, the small hardware platforms are colloquially referred to as *smart dust* and/or *motes* because of their miniature size. The research community has enthusiastically embraced WSNs—for example, see articles on *ambient intelligence* by Basten et al. 2003 and Mukherjee et al. 2006; and the well-known *Scientific American* article written by M. Weiser (1991) on *ubiquitous computing*. This enthusiasm has consequently spurred the commercial availability of the hardware platforms and system software, such as TinyOS (Hill and Culler 2002). New companies have been formed around the technology and successful prototype systems have been installed for low duty-cycle temperature monitoring in commercial buildings where radio transmission is relatively robust (see Conner 2006 for a list of commercial websites). Such 'early adopters' will hopefully create experience and know-how that will facilitate the wider adoption of wireless sensor networks. Even in non-manufacturing settings (for example, the energy monitoring in buildings)

A review of WSN applications and IoT applications

[1]PRIYANSU CHANDAN BEHERA,
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]PRAHALLAD PRADHAN,
Samanta Chandra Sekhar Institute of Technology & Management, Koraput, Odisha, India

Abstract— *With advancements in wireless technology and digital electronics, some small devices have begun to be used in a variety of everyday situations. These devices have the ability to sense, compute, and communicate. They are typically made up of low-power radios, a number of smart sensors, and embedded CPUs (Central Processing Units). These devices are used to create a wireless sensor network (WSN), which is required for sensing services and monitoring environmental conditions. Parallel to WSNs, the concept of internet of things (IoT) is being developed, where IoT can be defined as an interconnection between identifiable devices in sensing and monitoring processes via an internet connection. This paper provides a comprehensive overview of WSNs. It also evaluates WSN technology and characteristics. It also includes a review.*

Index Terms— **Wireless Sensor Networks, Internet of Things, Sensor Node, Ad-hoc Network, WSN Security, IoT.**

I. Introduction

WITH the rapid technological development of wireless technology and embedded electronics, Wireless Sensor Networks (WSNs) have started to attract researchers' interest. A typical WSN is composed of tiny devices which are known as nodes. These nodes include embedded CPU, limited computational power and some smart sensors. With these sensors, Nodes are used to monitor surrounding environmental factors such as humidity, pressure, heat and vibration. Typically, a node in any WSN contains sensor interface, computing unit, transceiver unit and power unit. These units perform crucial tasks by making nodes able to communicate among each other to transmit data obtained by their sensors. Communication between the nodes is necessary to have a centralized system. The necessity of this system leads to development of the notion of internet of things (IoT). With the notion of IoT, immediate access to environmental data becomes feasible. So that in numerous processes, efficiency and productivity increases dramatically.

In this paper, a detailed overview of WSNs is given. The objectives of this paper are assessing WSNs technology and characteristics, reviewing WSNs applications and providing information on the challenges and future of WSNs. Section2 starts with the definition of WSNs and it provides the architecture of WSNs. Section3 gives historical background of WSNs and Section4 explains how WSNs work. In Section5 advantages and disadvantages of WSNs are listed. Section6 provides information on application of WSNs and Section7 addresses the challenges of WSNs security and privacy. Lastly, Section 8 addresses the future trends of WSNs and IoT applications.

II. What is a WSN?

Typically, a WSN can be defined as a network of nodes that work in a cooperative way to sense and control the environment surrounding them. These nodes are linked via wireless media. Nodes use this connection to communicate among each other. The architecture of a typical WSN consists of following 3 components: sensor nodes, gateway and observer (user). Sensor nodes and gateways constitute the sensor field. Gateways and observers are interconnected via special networks or more commonly via internet (please see Fig. 1).

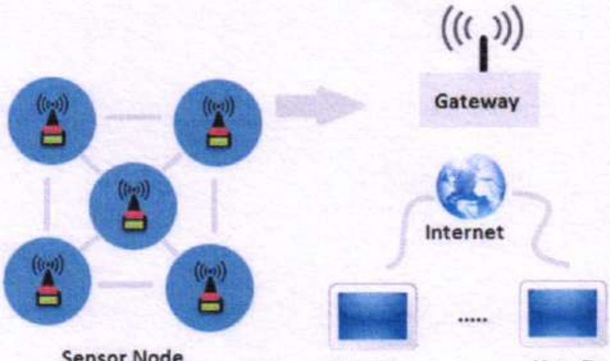


Fig. 1. Wireless Sensor Network (WSN)

Conceptually a WSN is based on a simple equation which

A brief survey Wireless Sensor Networks to Automobiles

[1]RAJAT MISHRA,

Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]GANESWAR ROUT,

PNS School Of Engineering & Technology, Kendrapara, Odisha, India

Some applications of Wireless Sensor Networks (WSNs) to automobiles are identified, and the use of Crossbow MICAz motes operating at 2.4 GHz with TinyOS support is considered. These WSNs are designed to measure, process, and provide various types of information to users while driving. Examples include acceleration and fuel consumption, identification of incorrect tyre pressure, illumination verification, and evaluation of the driver's vital signals. A brief overview of WSN concepts is provided, as well as the development of the wireless sensor network itself. Calibration curves were created, allowing for the measurement of luminous intensity and temperature in the appropriate units. Aspects of architecture definition and protocol selection/implementation are discussed.

Keywords: wireless sensor networks, applications, MICAz motes, automobile, architectures, protocols

1. INTRODUCTION

NOWADAYS, the need to collect, interpret and act on real-time data gains increasing interest. However, to collect data using typical wired sensor networks has always been expensive, owing to installation and maintenance costs, and is limited in its range.

Although past wireless measurement solutions have been elusive, the spreading of the use of wireless sensor networks (WSNs) is in fast development. WSN is a term used to describe an emerging class of embedded communication products that provide redundant, fault-tolerant wireless connections between sensors, actuators and controllers. The large amount of research projects in this area allows for the existence of better tiny hardware devices with reduced cost/size, and improvements in software performance. WSNs are typically formed by groups of several sensor nodes, the so-called motes, whose individual constitution is based on actually combining sensor radios and CPUs into an effective robust, secure and flexible network, with low power consumption and advanced communication and computation capabilities, one or more sensors, a communication device (typically a radio), a microcontroller (with memory) and a power supply (battery). Its applications include industry, atmosphere monitoring, and defence, among others. Besides instrumentation concepts, WSNs involve aspects of wireless communications, networks architectures, and protocols.

Due to technological innovations in the area of wireless communications, digital electronics, and personal micro-electromechanical systems, a revolution is occurring in the area of measurement with remote wireless sensors [1]. In particular, WSNs are characterised by a high amount of sensor nodes with multi-hop communication capabilities. These tiny sensors can be spread inside the environment to be monitored or close to it, with positions that are not pre-determined. Indeed, they are set randomly as wireless sensors can be dropped onto places with difficult access from helicopters or airplanes [1]. These motes exchange messages among each other in order to efficiently monitor an environment/process, and operate while balancing the trade-off between low energy consumption and the need to fulfil the assigned tasks.

The application of wireless sensor networks to the automobile constitutes a challenge to be faced in this endeavour; we conceived a wireless sensor system capable to collect, process and supply several types of technical information (to the user) during an automobile journey. The examples are acceleration and fuel consumption, identification of wrong tires pressure value, acknowledgment of illumination failures (turn lights, brake lights, front lights, and register plate lights), and determination of the vital signals of the driver. We chose Crossbow MICAz sensors operating at 2.4GHz (IEEE 802.15.4), and supported by TinyOS. The concepts and the wireless sensor network itself (transmitter/receiver/ interface board) are explained, and aspects of the architecture, and of the implementation of the protocols itself are established. Security aspects are also addressed, and the power consumption issues are discussed.

Section 2 discusses some characteristics of WSNs and their applications to automobile industry, security services, military, environment, and medicine. In Section 3, routing protocols are briefly discussed, security aspects and imperfections are presented, and energy consumption issues are addressed. In Section 4 the use of TinyDB is discussed. Section 5 presents the various components, e.g., flow, tyre pressure, light, acceleration, temperature, heart beat frequency, and blood pressure sensors. Relevant results are presented, e.g., for luminous intensity, temperature and arterial pressure, where the discussion includes the production of the calibration curves. Finally, conclusions are presented in Section 6.

Challenges of Wireless Sensor Networks and the Internet of Things

[1]RASHMI RANJAN SETHY,
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]PURASTAM BEHERA,
Samanta Chandra Sekhar Institute of Technology & Management, Koraput, Odisha, India

Abstract— *Wireless sensor networks (WSNs) are becoming more prevalent in our daily lives. They are being used in a variety of domains, including health-care, assisted and enhanced-living scenarios, industrial and production monitoring, control networks, and many others. WSNs are expected to be integrated into the "Internet of Things" in the future, where sensor nodes dynamically join the Internet and use it to collaborate and accomplish their tasks. However, when WSNs are integrated into the Internet, we must thoroughly investigate and analyse the issues that arise. We evaluate various approaches to integrating WSNs into the Internet in this paper and outline a set of challenges that we hope to address in the near future.*

INTRODUCTION

The future Internet, designed as an "Internet of Things" is foreseen to be "a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols" [1]. Identified by a unique address, any object including computers, sensors, RFID tags or mobile phones will be able to dynamically join the network, collaborate and cooperate efficiently to achieve different tasks. Including WSNs in such a scenario will open new perspectives. Covering a wide application field, WSNs can play an important role by collecting surrounding context and environment information. However, deploying WSNs configured to access the Internet raises novel challenges, which need to be tackled before taking advantage of the many benefits of such integration.

The main contributions of this paper can be summarized as follows: We look at WSNs and the Internet holistically, in line with the vision where WSNs will be a part of an Internet of Things. Thereby, we identify representative application scenarios for WSNs (see Section II) from the multidimensional WSN design space [2], in order to obtain insights into issues involved with the integration. These representative application scenarios open up different schemes for integrating the WSNs into the Internet, which we present and compare in Section III. A closer investigation of the integration possibilies then helps us identify critical challenges (see Section IV), which need to be addressed if the full potential of the integration of WSNs and the Internet has to be realized. Finally, in Section V we summarize our discussion, giving pointers for possible solutions to address the identified challenges while regarding the resource limitations present in common WSN nodes.

I. SELECTED WSN APPLICATIONS

The wide wireless sensor network application field can be divided into three main categories according to [3]: Monitoring space, monitoring objects and monitoring interactions between objects and space. The proposed classification can be extended by an additional category monitoring human beings.

One example of the first category is environmental monitoring. WSNs are deployed in particular environments including glaciers [4], forests [3], and mountains [5] in order to gather environmental parameters during long periods. Temperature, moisture or light sensor readings allow analyzing environmental phenomena, such as the influence of climate change on rock fall in permafrost areas [5].

The second category centers on observing particular objects. Structural monitoring is one of the possible illustrations of this category. By sensing modes of vibration, acoustic emissions and responses to stimuli, mechanical modifications of bridges [6] or buildings [7] indicating potential breakages of the structure may be detected.

Monitoring interaction between objects and space is the combination of both previous categories and includes monitoring environmental threats like floods [8] and volcanic activities [9].

Presenting an extension to the presented classification, the last category focuses on monitoring human beings. Worn close to the body, the deployed sensors can gather acceleration information and physiological parameters like heart beat rate. Especially in applications in the medical area, such deployments may help diagnosing bipolar patients [10] and monitoring elderly people in a home care scenario [11].

The proposed classification, and particularly the selected deployments, illustrate the high diversity of WSN applications in term of monitored subjects and environments. Beneficial for the Internet of Things, this important scenario diversity must however be taken into account by considering suitable approaches for the WSN integration into the Internet.

II. INTEGRATION APPROACHES

Connecting WSNs to the Internet is possible in the three main approaches mentioned by [12], differing from the WSN integration degree into the Internet structure. Currently adopted by most of the WSNs accessing the Internet, and

Research Issues for Wireless Sensor Networks: A Review

[1]SMITA RANI PADHY,
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]SAMARESH MANDAL,
PNS School Of Engineering & Technology, Kendrapara, Odisha, India

Abstract

Wireless sensor networks (WSN) are currently gaining popularity due to their limitless potential. However, such systems are still in their early stages, and many research challenges remain. In this short article, I will focus on six major research challenges for wireless sensor networks. I conclude by mentioning a few other research challenges that must be addressed before WSN becomes widespread.

Real-world Protocols:

Many current WSN solutions are developed with simplifying assumptions about wireless communication and the environment, even though the realities of wireless communication and environmental sensing are well known. Many of these solutions work very well in simulation. It is either unknown how the solutions work in the real world or they can be shown to work poorly in practice. We note that, in general, there is an excellent understanding of both the theoretical and practical issues related to wireless communication. For example, it is well known how the signal strength drops over distance. Effects of signal reflection, scattering and fading are understood. However, when building an actual WSN, many specific system, application, and cost issues also affect the communication properties of the system. Radio communication in the form of AM or FM broadcast from towers performs quite differently than short range, low power wireless found in self-organizing WSNs. Of course, while the same basic principles apply, the system performance characteristics vary considerably. In other words, the size, power, cost constraints and their tradeoffs are fundamental constraints. In the current state of the art, the tradeoff among these constraints has produced a number of devices currently being used in WSNs. For example, one such device is the Mica mote that uses 2 AA batteries, a 7 MHz microcontroller, an RF Chipcon radio, and costs about $100. As better batteries, radios, and microcontrollers become available and as costs reduce, new platforms will be developed. These new platforms will continue to have tradeoffs between these parameters.

Novel network protocols that account for the key realities in wireless communication are required. New research is needed to:

> Measure and assess how the theoretical properties of wireless communication are exhibited in today's and tomorrow's sensing and communication devices,
> Establish better models of communication realities to feed back into improved simulation tools,
> Invent new network protocols that account for the communication realities of real world environments,
> Test the individual solutions on real platforms in real world settings, and
> Synthesize novel solutions into a complete system-wide protocol stack for a real application.

Real-Time:

WSN deal with real world environments. In many cases, sensor data must be delivered within time constraints so that appropriate observations can be made or actions taken. Very few results exist to date regarding meeting real-time requirements in WSN. Most protocols either ignore real-time or simply attempt to process as fast as possible and hope that this speed is sufficient to meet deadlines. Some initial results exist for real-time routing. For example, the RAP protocol [1] proposes a new policy called velocity monotonic scheduling. Here a packet has a deadline and a distance to travel. Using these parameters a packet's average velocity requirement is computed and at each hop packets are scheduled for transmission based on the highest velocity requirement of any packets at this node. While this protocol addresses real-time, no guarantees are given. Another routing protocol that addresses real-time is called SPEED [2]. This protocol uses feedback control to guarantee that each node maintains an average

Opportunities and Challenges of Wireless Sensor Networks in Smart Grid: A Review

[1]SOUMYA PRADHAN,
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]PRASANNA KUMAR PRUSTY,
Samanta Chandra Sekhar Institute of Technology & Management, Koraput, Odisha, India

Abstract— *Wireless sensor networks (WSNs) have significant advantages over traditional communication technologies used in today's electric power systems due to their collaborative and low-cost nature. WSNs have recently been widely recognised as a promising technology that can improve various aspects of today's electric power systems, including generation, delivery, and utilisation, making them an essential component of the smart grid, the next-generation electric power system. The harsh and complex electric-power-system environments, on the other hand, pose significant challenges to the reliability of WSN communications in smart-grid applications. This paper begins with an overview of the application of WSNs for electric power systems, including opportunities and challenges, and then moves on to future work in many unexplored research areas in diverse smart-grid applications. Following that, it presents a comprehensive experimental study on statistical approach.*

Index Terms—**CC2420, diagnostics, IEEE 802.15.4, link-quality indicator (LQI), monitoring, received signal strength indicator (RSSI), smart grid, wireless sensor networks (WSNs).**

I. Introduction

THE global climate change and rapidly growing populations over the past decades have generated increasing demands for abundant, sustainable, and clean electric energy on a global basis. However, in most countries today, the increasing energy demand means an even heavier burden on the already overstressed, overaged, and fragile electricity infrastructure. In the U.S., for example, the average age of power-grid transmission lines is beyond 50–60 years [29]. Over the last 20 years, the electricity demand and consumption have increased continuously by 2.5% annually according to a U.S. Department of Energy report [8]. The increasing electricity demand, together with the complex and nonlinear nature of the electric power distribution network, have caused serious network congestion issues. The network congestion and safety-related factors have become the main causes of several major blackouts that happened in recent years. In addition to the overstressed situation, the existing power grid also suffers from the lack of pervasive and effective communications, monitoring, fault diagnostics, and automation, which further increase the possibility of region-wide system breakdown due to the cascading effect initiated by a single fault. Furthermore, the global increasing adaptation of renewable and alternative energy sources in the 21st century also introduced new issues, such as power-grid integration, system stability, and energy storage, which also need to be addressed as additional challenges.

To address these challenges, a new concept of next-generation electric power system, a *smart grid*, has emerged. The smart grid is a modern electric power-grid infrastructure for improved efficiency, reliability, and safety, with smooth integration of renewable and alternative energy sources, through automated control and modern communication technologies [2], [5]. In the smart grid, reliable and online information becomes the key factor for reliable delivery of power from the generation units to the end users. The impact of equipment failures, capacity limitations, and natural accidents and catastrophes, which cause power disturbances and outages, can be largely avoided by online power system condition monitoring, diagnostics, and protection. In this respect, the intelligent and low-cost monitoring and control enabled by online sensing technologies have become essential to maintain safety, reliability, efficiency, and uptime of the smart grid [11], [13], [19], [30].

Traditional electric-power-system monitoring and diagnostic systems are typically realized through wired communications. However, the wired monitoring systems require expensive communication cables to be installed and regularly maintained, and thus, they are not widely implemented today because of their high cost [7]. Hence, there is an urgent need for cost-effective wireless monitoring and diagnostic systems that improve system reliability and efficiency by optimizing the management of electric power systems [11], [13].

As one of the main objectives, this paper gives a first glimpse and opens up future work in many unexploited research areas of applying wireless sensor networks (WSNs) in smart grid by providing an overview of the opportunities and challenges. The collaborative operation of WSNs brings significant advantages over traditional communication technologies, including rapid deployment, low cost, flexibility, and aggregated intelligence