Faisal Karim Shaikh
Bhawani Shankar Chowdhry
Habib M. Ammari
Muhammad Aslam Uqaili
Asadullah Shah (Eds.)

Communications in Computer and Information Science 366

Wireless Sensor Networks for Developing Countries

First International Conference, WSN4DC 2013
Jamshoro, Pakistan, April 2013
Revised Selected Papers

Springer

Communications in Computer and Information Science 366

Faisal Karim Shaikh Bhawani Shankar Chowdhry
Habib M. Ammari Muhammad Aslam Uqaili
Asadullah Shah (Eds.)

Wireless Sensor Networks for Developing Countries

First International Conference, WSN4DC 2013
Jamshoro, Pakistan, April 24-26, 2013
Revised Selected Papers

Springer

Volume Editors

Faisal Karim Shaikh
Mehran University of Engineering and Technology, Jamshoro, Pakistan
E-mail: faisal.shaikh@faculty.muet.edu.pk

Bhawani Shankar Chowdhry
Mehran University of Engineering and Technology, Jamshoro, Pakistan
E-mail: c.bhawani@ieee.org

Habib M. Ammari
University of Michigan-Dearborn, MI, USA
E-mail: hammari@umd.umich.edu

Muhammad Aslam Uqaili
Mehran University of Engineering and Technology, Jamshoro, Pakistan
E-mail: pvc@admin.muet.edu.pk

Asadullah Shah
International Islamic University, Malaysia
E-mail: asadullah@iium.edu.my

ISSN 1865-0929 e-ISSN 1865-0937
ISBN 978-3-642-41053-6 e-ISBN 978-3-642-41054-3
DOI 10.1007/978-3-642-41054-3
Springer Heidelberg New York Dordrecht London

Library of Congress Control Number: 2013948110

CR Subject Classification (1998): C.2, H.4, I.2, H.3, D.2, K.6.5, J.1-2, H.5

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

This book constitutes the refereed proceedings of the First International Conference on Wireless Sensor Networks for Developing Countries, WSN4DC 2013. With the emergence of electronics and nanotechnology, pervasive and ubiquitous environments are becoming a reality. The key enabler technology for these environments is wireless sensor networks (WSNs). We have seen several WSN advancements recently in the military domain. The world is now well aware of the power of WSN and its applications, which are endless. WSN4DC aims to bring together a wide spectrum of international experts to facilitate a creative environment for the promotion of collaboration and knowledge transfer under the domain of WSN usage for developing countries. In particular, WSN4DC facilitates a dialog between major industry players, entrepreneurs, and academia to help create a road-map for the development of tangible research environment in developing countries. WSN4DC is an international forum for researchers to exchange information regarding novel aspects of technology, application, and service development within the WSN domain.

This year, WSN4DC 2013 received 30 submissions. A small subset of papers was classified as quick rejects based on their quality and likelihood of acceptance. All the other papers underwent a rigorous review process with each paper receiving at least three reviews. The review process comprised several stages including Technical Program Committee (TPC) member reviews, TPC lead summary recommendations, and additional reviews (as needed). Based on the TPC recommendations, we were only able to accept ten papers for publication and presentation at WSN4DC 2013. This represents an acceptance rate of approximately 33%. The conference program was structured into two parallel-track sessions for the presentation of papers, a track for short paper presentation, a PhD Symposium, and a Poster Session. The topics presented had a reasonable balance between theory and practice in WSNs. The program also included three keynote speeches by renowned experts in the field, and two parallel thematic tutorials.

This event would not have been possible without the enthusiastic and hard work of a number of colleagues. We would like to express our gratitude to the General Chairs, for their assistance through the whole process, and the Steering Committee members for their supportive guidance. We also thank all the other members of the Organizing Committees for the fruitful cooperation. A special thanks goes to the TPC members, and all the referees, for their invaluable help in reviewing the papers. We would also like to thank our partners and sponsors, especially the Higher Education Commission, National ICT R&D Fund, and

Pakistan Science Foundation. We wish to acknowledge all the authors for their overwhelming support in submitting their papers to WSN4DC 2013. Last but not least, we wish to thank all the participants for attending the conference.

April 2013

Faisal Karim Shaikh
Bhawani Shankar Chowdhry
Habib M. Ammari
Asadullah Shah
M. Aslam Uqaili

Conference Organization

Conference Chairs

Abdul Qadeer K. Rajput	MUET, Pakistan
Rahman	City University London, UK
Tengku Mohd Bin Tengku Sembok	IIUM, Malaysia
M. Aslam Uqaili	MUET, Pakistan

Steering Committee

Giuseppe Anastasi	University of Pisa, Italy
Nirwan Ansari	New Jersey Institute of Technology, USA
Xiuzhen Cheng	The George Washington University, USA
Tariq S. Durrani	University of Strathclyde, UK
Wendi Heinzelman	University of Rochester, USA
Mingyan Liu	University of Michigan Ann Arbor, USA
Steve Olariu	Old Dominion University, Norfolk, USA
Sethuraman Panchanathan	Arizona State University, USA
Ramjee Prasad	Aalborg University, Denmark
Ryszard Struzak	NIT, Poland/ICTP, Italy
Neeraj Suri	TU Darmstadt, Germany
Niel M. White	University of Southampton, UK
Jie Wu	Temple University, USA

Technical Program Committee Chairs

Faisal Karim Shaikh	MUET, Pakistan
Bhawani S. Chowdhry	MUET, Pakistan
Habib M. Ammari	Univ. Michigan-Dearborn, USA
Asadullah Shah	IIU, Malaysia

Publicity Chairs

Habib M. Ammari	University of Michigan-Dearborn, USA
Faisal Karim Shaikh	MUET, Pakistan

Local Chairs

Aftab A. Memon	MUET, Pakistan
Mukhtiar A. Unar	MUET, Pakistan

Poster Session Chairs

Faheem Umrani	MUET, Pakistan
Zafi Shah	MUET, Pakistan

Phd Symposium Chairs

Imran Jokhio	MUET, Pakistan
Nafeesa Zaki	MUET, Pakistan

Tutorial Chairs

Sana Hoor Jokhio	MUET, Pakistan
Sania Bhatti	MUET, Pakistan

Registration and Management Committee

Attia Baqai	MUET, Pakistan
Hyder Bux	MUET, Pakistan
Irfan Halepota	MUET, Pakistan
Shakeel Laghari	MUET, Pakistan
Sajjad Memon	MUET, Pakistan
Jibran Memon	MUET, Pakistan
Zubair Memon	MUET, Pakistan
Umair Quereshi	MUET, Pakistan
Mohsin Shah	MUET, Pakistan
Mehran Memonai	MUET, Pakistan

Web and Local Publicity Committee

Mustafa Baloach	MUET, Pakistan
Khurram Bhatti	MUET, Pakistan
M. Murtaza Chang	MUET, Pakistan
Ashfaque Issani	MUET, Pakistan
Saadullah Kalwar	MUET, Pakistan
Ahsan Memon	MUET, Pakistan
Agha Aadil	MUET, Pakistan

Finance Committee

Aftab Ansari	MUET, Pakistan
Zeeshan Memon	MUET, Pakistan
Munir A. Shaikh	MUET, Pakistan

Program Committee

Muhammad Aamir	Sir Syed University of Engineering & Technology, Karachi, Pakistan
Arshad Ali	National University of Since and Technology, Islamabad, Pakistan
Azad Ali	Technical University of Darmstadt, Darmstadt
Zeeshan Ali	Mehran University of Engineering and Technology, Jamshoro, Pakistan
Habib Ammari	University of Michigan-Dearborn, USA
Adnan Ashraf	Mehran University of Engineering and Technology, Jamshoro, Pakistan
Javed Baloch	Mehran University of Engineering and Technology, Jamshoro, Pakistan
Sania Bhatti	Mehran University of Engineering and Technology, Jamshoro, Pakistan
Arabella Bhutto	MUISTD, Mehran University of Engineering and Technology, Jamshoro, Pakistan
Nafeesa Bohra	Mehran University of Engineering and Technology, Jamshoro, Pakistan
Safdar Hussain Bouk	COMSATS Institute of Information Technology, Islamabad, Pakistan
Mehmet Can Vuran	University of Nebraska-Lincoln, USA
Qing Cao	University of Tennessee, USA
Xiuzhen Cheng	The George Washington University, USA
Bharat Chowdhry	IIIT, India
Flavia Delicato	Federal University of Rio de Janeiro, Brazil
Xinwen Fu	University of Massachusetts Lowell, USA
Jinhua Guo	University of Michigan-Dearborn, USA
Nick Harris	Univ. of Southampton, UK
Zahid Hussain	Technical University Graz, Institute for Software Technology, Austria
Jörg Hähner	Augsburg Uni, Germany
Imran Ali Jokhio	Mehran University of Engineering and Technology, Jamshoro, Pakistan
Sana Jokhio	Mehran University of Engineering and Technology, Jamshoro, Pakistan
Pardeep Kumar	Quaid-e-Awam Uni, Pakistan
Qilian Liang	University of Texas at Arlington, USA
Benyuan Liu	University of Massachusetts Lowell, USA
Yasir Arfat Malkani	University of Sindh, Jamshoro, Pakistan

Tommaso Melodia	State Univ. of New York at Buffalo, USA
Sheeraz Memon	Mehran University of Engineering and Technology, Jamshoro, Pakistan
Syed Misbahuddin	Sir Syed University of Engineering and Technology, Karachi, Pakistan
Parag Mogre	Siemens AG, Germany
Christian Poellabauer	University of Notre Dame, USA
Nadia Qadri	COMSATS Institute of Information Technology, Pakistan
Christian Renner	Luebeck Univ., Germany
Faisal Karim Shaikh	Mehran University of Engineering and Technology, Jamshoro, Pakistan
Bhawani Shanker	Mehran University of Engineering and Technology, Jamshoro, Pakistan
Cormac Sreenan	Univ. College Cork, Ireland
Aaron Striegel	University of Notre Dame, USA
Fahim Umrani	Mehran University of Engineering and Technology, Jamshoro, Pakistan
Thiemo Voigt	Uppsala University, Sweden
Shengquan Wang	University of Michigan-Dearborn, USA
Yuehua Wang	Wayne State Univ., USA
Wendong Xiao	University of Science and Technology Beijing, China
Mohamed Younis	University of Maryland Baltimore County, USA
Marco Zennaro	ICTP, Italy

Additional Reviewers

Javaid, Nadeem
Li, Wei
Liao, Jilong
Minhas, Abid Ali
Qureshi, Rehan
Sarkar, Dr Jahangir
Shamsi, Dr Jawwad

Organizer

Mehran University of Engineering & Technology, Jamshoro
PAKISTAN

In Collaboration

Erasmus Mundus STRoNG TiES

الجامعة الإسلامية العالمية ماليزيا
INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

Sponsors

National ICT Fund, Pakistan

Higher Education Commission, Pakistan

Pakistan Science Foundation

Table of Contents

Development of a Low-Power Smart Water Meter for Discharges in Indus Basin Irrigation Networks*

Zahoor Ahmad[1], Ehsan U. Asad[1], Abubakr Muhammad[1],
Waqas Ahmad[2], and Arif Anwar[2]

[1] Department of Electrical Engineering, SBA School of Science & Engineering, LUMS,
Lahore, Pakistan
{zahoor.ahmad,ehsan.haq,abubakr}@lums.edu.pk
[2] International Water Management Institute (IWMI) Pakistan Office, 12km Multan Road,
Lahore, Pakistan
{a.anwar,w.ahmad}@cgiar.org

Abstract. To improve the sampling frequency of water diversion to distributary canals and to improve equity of distribution and data handling we have developed a smart electronic water meter based on ultrasonic sensors and GPRS modem to frequently record and transmit the water diversion data to a centralized server. The server processes the data to extract useful information for example seasonal cumulative water deliveries and discharge time series. The Wireless Sensor Node (WSN) inspired design is extremely low-power, field deployable and scalable with respect to cost and numbers. This paper, reports the first steps towards practical realization of a smart water grid in the Indus river basin, conceptualized by the authors in previous theoretical studies.

Keywords: Hydrometry, Wireless Sensor Networks, Water management.

1 Introduction

The Indus River Basin in Pakistan has the world's largest contiguous irrigation network, running over 90,000 Km of watercourses and around 25 million acre irrigated area, the overall irrigation infrastructure accounts for approximately US$ 300 billion. Such a large system cannot be managed with high efficiency without using unprecedented levels of automation and usage of decision support systems [1],[3],[11]. Quite contrary, most of the operation is manual which combined with poor management practices have contributed towards acute problems of water scarcity and distribution inequity. Refer [2] and [6] for an overview of such problems. Therefore, there is a great need to contribute towards agricultural development in Pakistan through the efficient management of surface water in canal networks to enhance food security, reduce poverty and adapt to uncertainties brought about by climate change.

* The authors would like to acknowledge financial support provided by the Embassy of the Kingdom of Netherlands, Islamabad, Pakistan through Grant #22294 used in part for the partnership between IWMI and LUMS to undertake the research described in this work.

F.K. Shaikh et al. (Eds.): WSN4DC 2013, CCIS 366, pp. 1–13, 2013.

Future irrigation networks as described by [4] and other leading researchers, represent a prime example of cyber physical systems (CPS), i.e. physical infrastructures coupled tightly with distributed networks of sensing, computing and control structures. Refer [7],[12] and [15] for a discussion on CPS. In the context of Indus river basin, the LUMS affiliated authors have conducted a series of theoretical studies to determine the feasibility of a fully automated CPS, envisioned as a smart water grid for Pakistan. Refer [9] and [14] as examples of such case studies. Encouraged by these studies, the group has come into several partnerships in recent years with government and non-government organizations to translate the theory into practical systems. The IWMI affiliated authors of this study have similarly been arguing for such automations in the context of wider governance issues related to participatory irrigation management, enforcement of water rights and accountability.

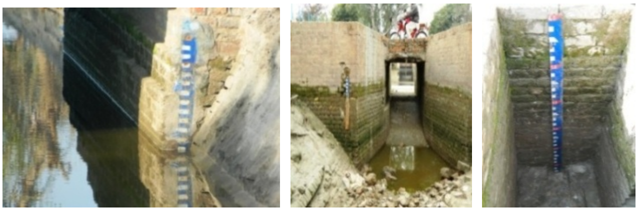


Fig. 1. Examples of manual gauge readout settings for *pansal nawisi* by Punjab Irrigation Department in Hakra Branch, Bahawalnagar. The water levels are converted to flow using a *rating curve* derived from channel geometry.

This paper focuses on automating the hourly-to-daily measurement of canal water discharges (pinsal nawisi) in the network (Refer Fig. 1). This is one of the most critical requirements of automation in the Indus basin due to the following reasons. First, the scale of such measurements, even at a local canal command is very large. The scale enormity when combined with the manual nature of daily flow measurements poses obvious logistical problems in data collection, dissemination and interpretation. Second, the fidelity of manual measurements is questionable due to deteriorating infrastructure and human factors in gauge reading. Third, there is a need to give near real-time picture to basin managers (the provincial irrigation departments, area water boards, farmer organizations) to perform situation assessment and planning, resolve conflicts, ensure transparency and maintain equity amongst users. The manual operation allows no quicker than daily updates. Fourth, automation can enable other operations and services that are not yet feasible such as volumetric metering, demand based delivery, detection of leakages and non-technical losses, structural health monitoring, re-planning under changing scenarios etc. Lastly, automated flow measurements will be the first step towards installing even higher levels of automation such as controlled gates and other active structures.

Keeping in mind these motivations, we have developed a fully functional, field deployable, stand alone and weather proof canal flow measurement system. The design is inspired from wireless sensor network (WSN) technology and most suitable for installation on branch canals and distributaries at irrigation canal networks of the

Indus river basin. At the time of writing, 24 nodes are being installed by the authors in Bahawalnagar, Punjab in the Hakra canal command area off the River Sutlej. A full analysis of the networked sensing system with data analysis and interpretation will be reported after testing the system for the upcoming Rabi and Kharif seasons. This paper mostly reports the development of electronics for the wireless sensor node, brief descriptions of the software backbone and supporting civil infrastructure.

A high level diagram of the proposed automation is shown in Fig. 2. A stilling well is constructed in close proximity to the canal. At the top of the stilling well is installed a battery powered wireless sensor node that samples the level of water using the principle of ultrasonic distance measurement. The measured water level is time-stamped and then transmitted to a central office at regular intervals using GPRS/GSM based services. Here, a computer server receives the raw water level data, calibrate them, convert them into discharge (in cubic feet per second, cfs) using a predefined rating curve and then file them in a database. Subsequently, the data is made available for dissemination in the form of graphs, time series and text using various standard web and mobile based services.

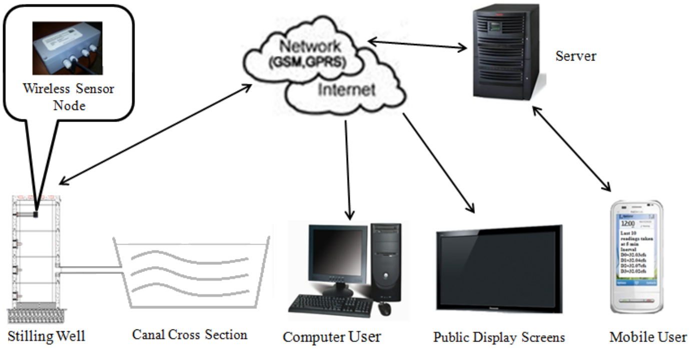


Fig. 2. System data flow diagram

The contributions of this article are as follows. Firstly, we achieve extremely low-power battery powered design providing a practical compromise between two extremes: A direct AC mains powered system which is infeasible at remote locations and a solar-powered system which is difficult to secure physically and adds significantly to the cost. Our design guarantees a long-life completely battery powered system only requiring low-cost annual battery replacement. Secondly, we successfully demonstrated usage of maintenance-free ultrasound based sensing instead of conventional mechanical floats or pressure transducers. We have selected extremely accurate, weather proof and narrow beam sensors to overcome installation difficulties within a stilling well. We have taken care to compensate for changes in speed of sound in weather exposed conditions. Thirdly, the unit is field deployable in that we have packaged, tested and calibrated the sensor for all extreme conditions. Though briefly touched in this article, real-world deployment challenges have been systematically tackled in software and civil infrastructure, making our system much more than a laboratory prototype.

2 Wireless Sensor Node Design

In this section, we will mainly focus on Wireless Sensor Node (WSN) (Refer Fig. 3). It consists of an ultrasonic range finder as the main sensor for measuring water level and flow. It also has capabilities to interface to auxiliary sensors such as a temperature sensor immersed into the water to calculate its temperature. In the future, we are planning to add other sensors to measure the turbidity and salinity of water. The system is operated with 3.6V, 14000mAH batteries with surge current capabilities. It also has a temperature sensor immersed into the water and calculates the temperature of the water. The WSN calculates the water level in the canal and sends the data to the server through GPRS/GSM at a predefined but configurable interval. Please refer to the block diagram shown in Fig. 4. The details of each important component are given below.

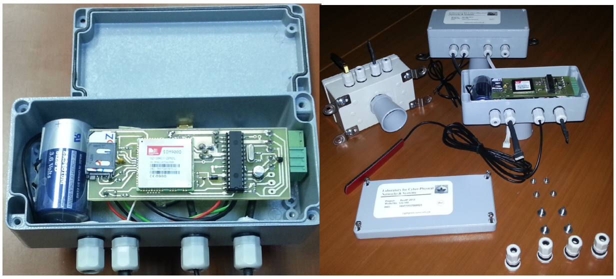


Fig. 3. Photographs of the developed Smart Water Meter

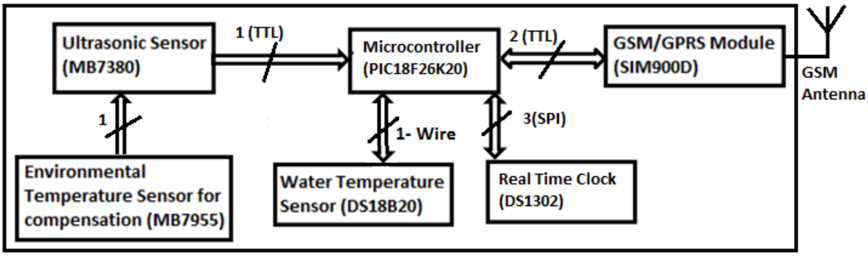

Ultrasonic Sensor (MB7380)
1 (TTL)
Microcontroller (PIC18F26K20)
2 (TTL)
GSM/GPRS Module (SIM900D)
GSM Antenna
1
1- Wire
3(SPI)
Environmental Temperature Sensor for compensation (MB7955)
Water Temperature Sensor (DS18B20)
Real Time Clock (DS1302)

Fig. 4. Block diagram of Wireless Sensor Node

2.1 Ultra Sonic Sensor

The Maxbotix MB7380 Ultra Sonic Sensor [8] is a cost-effective solution for applications where precision range-finding, low voltage operation, space saving, low-cost and IP67 weather resistance rating is needed. Each time the sensor takes a range reading, it calibrates itself. The sensor then uses this data to range objects. This sensor line features 1-mm resolution, target-size and operating-voltage compensation for improved accuracy and internal speed-of-sound temperature compensation. To correct power related noise issues we added a 100uF capacitor at the sensor between the V+ and GND pins. The speed of sound in air increases about 0.6 meters per second, per degree centigrade. If the temperature, humidity, or applied voltage changes during sensor operation, the sensor will apply necessary temperature and voltage compensations. Although the MB7380 has an internal temperature sensor; for best accuracy, we used the optional external temperature sensor MB7955 which is detected automatically and compensations are applied for temperature variations in acoustic ranging path.

MB7380 sensor has a calibrated beam pattern. Beam pattern is a 2D representation of the detection area of the sensor. The beam pattern is actually shaped like a 3D cone. Beam pattern is used for a specific target at any given distance to calculate the beam angle for that target at the specific distance. Generally, for shorter distances we need narrower beam angle. Our expected distance to be measured is 1-2 meters. So the cone does not interfere with the walls of the stilling well.

2.2 Microcontroller

Microchip's PIC18F26K20 flash microcontroller with extreme low power (XLP) is used in our embedded design. It is featured with up to 64 kbytes of linear program memory addressing, 1024 bytes of EEPROM data and up to 3936 bytes linear data memory addressing. Each data sample is time stamped which makes it 8 bytes long. We save the most recent 110 records in non-volatile EEPROM and the remaining 500 records in the volatile SRAM. We take the sample after 30 minutes intervals, so we have a total of 48 records daily. Thus, with this much memory we can save 12 days data in case of GPRS/GSM transmission problems.

2.3 GPRS/GSM Module

We used SIMCOM SIM900D Version 1.03 for GPRS/GSM transactions. SIM900D [13] is a quad-band GPRS/GSM engine that works on GSM frequencies. The module is integrated with the TCP/IP protocol; extended TCP/IP AT commands are developed for reliable data transfer applications. The module has GPRS data and transfer of 42.8 kbps. The manufacturer claims the module to be working from 3.1V to 4.8V, but practically we found that the module is not getting itself registered with the network below 3.4V.

2.4 Extreme Low Power Design

As our application require prolonged standalone operation. We are planning our system to last for up to 5 to 10 years, while running from a single battery. To enable applications like these, we selected products with Microchip's nanoWatt XLP Technology, offering the lowest currents for run and sleep. We worked to design the system such that it does not require any maintenance over the lifespan of the application. The designed hardware is spending 98% of its time in sleep. We are powering the circuitry with 3.6V, 14,000mAH Lithium Thionyl Chloride Batteries. Fig. 5 shows typical discharge characteristics at various current levels. A 100µF low ESR tantalum capacitor is placed across the battery, which causes the current spike of 1-2 Amperes (few milliseconds wide) during transmission burst to smooth down to 200-300mA (2 to 3 seconds wide). We cannot run it with normal Lithium Ion Cells, because they have lower surge currents.

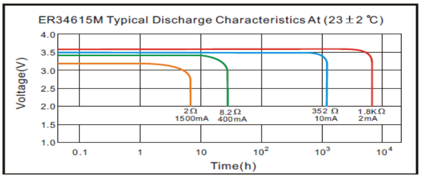


Fig. 5. Battery Discharge Characteristics Refer [5]

GSM/GPRS transactions consume most of the battery power. We turn the GSM module off after every transaction which takes 30uA at shutdown mode. Also the sensors are turned on only at sampling time. In this section, we will highlight the various extreme low-power control features of an embedded microcontroller. The microcontroller might have nothing else to do until the peripheral collects a certain amount of samples. Therefore, the microcontroller enters "sleep" in between each data sample. We evaluated the time×current elements of the energy equation and determined best option is to operate the MCU for longer at low frequency, because the MCU is in running mode during transaction for most of the time. During that time the GSM needs some delays to get registered with the network.

Fig. 6 shows current consumed for a single GPRS transaction. It would be worth mentioning here that currents consumed during GPRS transactions, varies greatly with RF signal strength. At low signal level WSN will consume more current during the transmission burst (Refer Fig. 7). While the GSM module is shut down for about one hour it takes 1-2 mA current. The sensors are on for only 2 seconds and take not more than 2mA current, so we are ignoring those currents and only consider currents consumed by GSM part of WSN. The graph specifies that the GSM module turns on at 7th second and after doing the transaction turns off after 100 seconds. At 16th second WSN registers itself with the GSM network. For the next 40 seconds it waits for an incoming text message. At 65th second the system brings up wireless connection with GPRS. After 74 seconds, WSN starts up a TCP connection. It makes two tries to get connected. At 85th second it sends the data successfully. It waits for an incoming data from the server and then shuts down the GSM part. Currents consumed by the microcontroller PIC18F26K20 (at 2.9V) in various modes boast sleep currents below 100 nA, Watch-dog Timer down to 1μA and Run-currents down to 100 μA/MHz. This essentially means that the GSM module should be the main focus of our design from the point of view of power consumption.

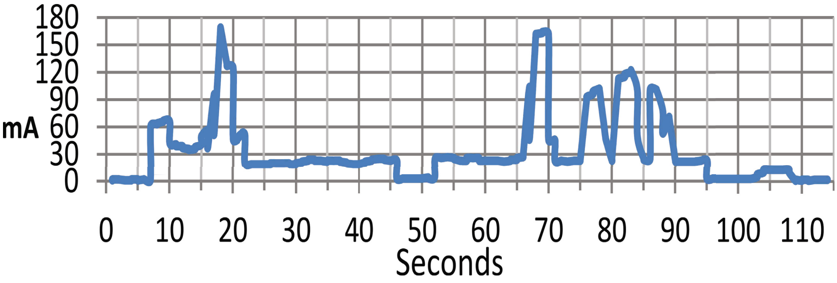


Fig. 6. Current vs. time plot for one transmission burst

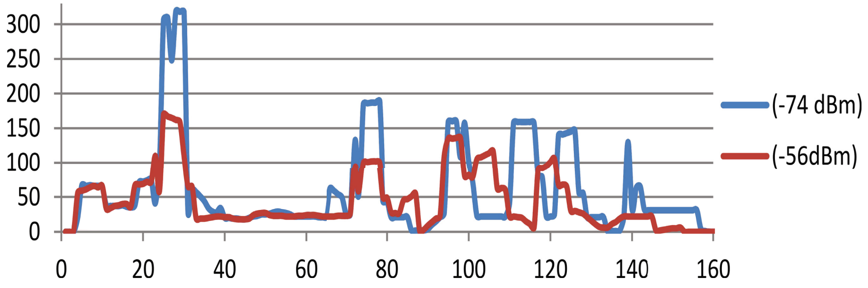


Fig. 7. Currents consumed at -74dBm and -56dBm signal levels

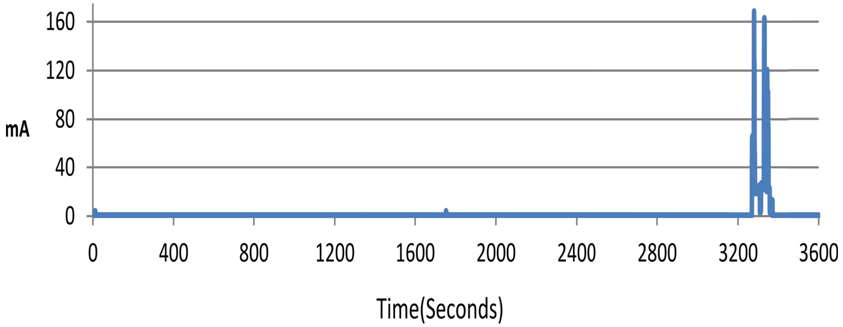


Fig. 8. Current Vs. Time plot for one transmission cycle (~one hour)

At sleep mode, WSN consumes 0.5-0.6 mA of current. Let us integrate the curve shown in Fig. 8 for an hour interval. We are using two batteries in parallel, so we have a total of 28AH charge.

$$q(T) = \int_0^T i(t)dt. \approx \sum_{n=0}^{3600} i(n).\Delta t = 6077mC = 6.077Coulomb.$$

Thus expected battery life = (28*60*60)/6.077=16,587Hours= 691 days. Please find the below results for burst transmission during various signal strength. The signal strength was varied by placing conductor materials around WSN. In each of the below results the current samples are taken at 0.5 seconds interval. The below results show that at strong signal strength, WSN consumes low current during the transmission burst.

2.5 Hardware Enclosure

The electronic Circuitry is protected against the environmental factors with IP67 (dust tight and protected against immersion) Ingress Protection standards die cast Aluminum Box of 180mmx80mmx60mm. Die cast Aluminum is selected because it is not corroded even if immersed in water. It has the capability to withstand harsh environmental conditions. The moisture and dust cannot enter inside the electronic circuitry. If the device is immersed into the water in case of flooding, the electronics will be protected. As GSM/GPRS signals do not work properly inside a metal housing. Four IP67 standard connectors are provided for antenna, two external temperature sensors (environment and water) and turbidity sensor in the future. The connectors are made of ABS plastic and are corrosion free with a special seal filled inside.

RoHS (Restriction of Hazardous Substances) Directive essentially states that electrical and electronic products put on the market shall not contain Lead, Cadmium, Mercury, Hexavalent Chromium, Poly brominated biphenyls and Poly brominated diphenylethers. All components and packing materials used in the design fulfill the requirement of RoHS.

2.6 Real Time Clock

Implementation of Real Time Clock (RTC) was necessary for Smart Water Meter to put a time stamp while take the reading. Dallas DS1302 was selected for its ease of availability and reliability. It consumes less than 500nA in battery backup and is operated with separate 3.3V 40mAH cell.

Thus, RTC cell backup time= (40mAH/500nA=80,000 hours=9 years). The RTC time can be checked and reset remotely from server side. RTC counts seconds, minutes, hours, date of the month, month, day of the week, and year with leap-year compensation valid up to 2100. It has three wire SPI interface and 8-pin SOIC package is used in our embedded design.

2.7 Design Problems and Their Solutions

Since Wireless Sensor Node is likely to be installed at locations with limited GSM/GPRS coverage. It is provided with an external antenna mounted at highest point inside the Stilling well. The device sends data on GPRS and in case of low RF signals it will initiate and SMS to the server, as SMS requires less signal strength.

Being operated from 3.6V battery, we are quite close to the minimum voltage ratings of SIM900D i.e., 3.4V.The copper traces from battery to the GSM module are 3.2 mm wide in the PCB design to reduce the voltage drop for situations, where the circuit consumes high currents like 1-2A during transmission burst. Note that $Resistance = (Resistivity{*}Length\ of\ wire)/Area.$ Also, wide tracks sink heat to the environment instantly. Narrow tracks result in high energy dissipation, which further increases the resistance in the absence of heat sink. Thus for best performance during transmission bursts we need to reduce the length of wire as well as widen copper traces on PCB from battery terminal to the GSM module. To appreciate the importance of this, note that SIM900D does not work below 3.4V. At high currents the voltage across the battery terminal decreases due to the internal resistance of the battery. If the resistance from battery terminal to the GSM module is 0.3 Ohm and we have a transmission burst of say 1.0A, then voltage drop across the wire, $V = IR = 1 * .3 = 0.3V$.So voltage at SIM900D will be 3.6V-0.3V=3.3V and will be powered down due to these drops.

The GSM part of WSN is protected against electro static discharge (ESD) with SMF05C, a 5 line transient voltage suppressor array, having a peak power dissipation of 100W (8 x 20 µS waveform) [10]. It has ESD rating of class 3B (exceeding 8 kV) per human body model and Class C (exceeding 400 V) per machine Model. Human body interaction with the circuitry is possible during SIM replacement. During assembling, we have ensured proper handling against electrostatic discharge. Anti-static Wrist Straps, are used to prevent ESD by safely grounding the technician working with electronic equipment. It consists of a band of fabric with fine conductive fibers woven into it.

2.8 Wireless Sensor Node Budget

The cost breakdown of the wireless sensor node has been given below from current list prices. Note, mainly that the absence of the solar panels have significantly reduced the unit price. Moreover, the maintenance is only annual replacement of batteries. We believe that this (low) cost has made the deployment of these units feasible at practical scales of deployment. Refer Table 1 below for budgeting details.

Table 1. WSN Budget

S.No.	ITEM	PRICE (USD)
1	MB7380 with temperature Sensor	114
2	SIM900D	20
3	Batteries	16
4	Die cast Aluminum Enclosure	26
5	Miscellaneous parts	14
	Total	$190 / PKR. 19,000

3 Software Design

3.1 Working

The WSNs installed at different canals send Water level readings on server. After the server receives the strings of data, it processes the data string and extracts the required parameters i.e., date, time, temperature, and level readings. These readings are then stored in the database with their respective date and time, which are then used to compute the seasonal cumulative water deliveries and discharge in average cubic feet per second (cfs). The data is displayed as CSV files with graphs depicting seasonal and yearly variations on a website. The whole software design consists of Server and Client side designs.

3.2 Server-Side Software Design

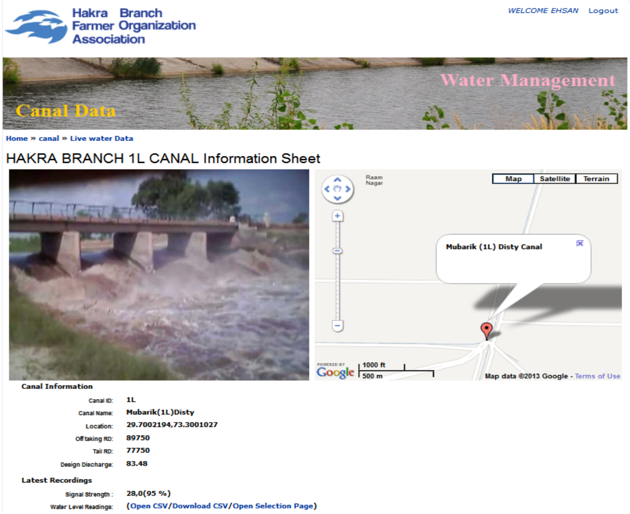
The Server side design comprises of Web Server, Server-side script, Operating System and a Database for storing the required data. Our choice for Server is the Microsoft Internet Information Services (IIS). We are using Microsoft server-side Web application framework (ASP.NET). For Relational Database Management System (RDBMS), we are using Microsoft SQL in web applications. The server is running on the Microsoft Window Server 2008 R2 Operating System.

The important aspects of the software design include:

1. **Security.** Common types of software flaws that lead to vulnerabilities include: SQL injection, Cross-site scripting and some others. MSSQL and Asp.net provides sufficient extensions and options to avoid such type of vulnerabilities.
2. **Replication and Back Up.** Replication of MSSQL database can be a solution to various problems like Scale-out problems, Data Security, Analytics, Long-distance data distribution and the Backup taken from slaves rather than from master, which result in no load on the production Master machine for this task. If the Slave node is down, this is not a problem since replication is performed asynchronously and when the Slave Node is up and Live after a downtime, it continues replication from the point it has been paused.

3.3 Client-Side Software Design

The design of the website is quite user-friendly and it provides users with an ease to check out the canal readings with the seasonal water discharge per unit area for different canals with other parameters like turbidity and temperature (Refer Fig. 9). The website is designed using the Hypertext markup language (HTML), Cascaded style sheet (CSS) for displaying and styling web pages. JavaScript, a commonly implemented as a part of a web browser, is used to create enhanced user interfaces and addition of some other features like Google map for showing the location of all the canals, drop down menu lists etc. Comma Separated Values (CSV) files is used to display the level readings. CSV files are practical for importing level readings into a spreadsheet programs like MS Excel. Fig. 10 shows a plot of the received readings from a test site over 19 hours, sampled at 10 minutes and transmitted from WSN at an interval of 1 hour.



HAKRA BRANCH 1L CANAL Information Sheet

Canal Information

Canal ID: 1L
Canal Name: Mubarik(1L)Disty
Location: 29.7002194,73.3001027
Off taking RD: 89750
Tail RD: 77750
Design Discharge: 83.48

Latest Recordings

Signal Strength : 28,0(95 %)
Water Level Readings: (Open CSV/Download CSV/Open Selection Page)

Fig. 9. Website User Interface for accessing the canal Information

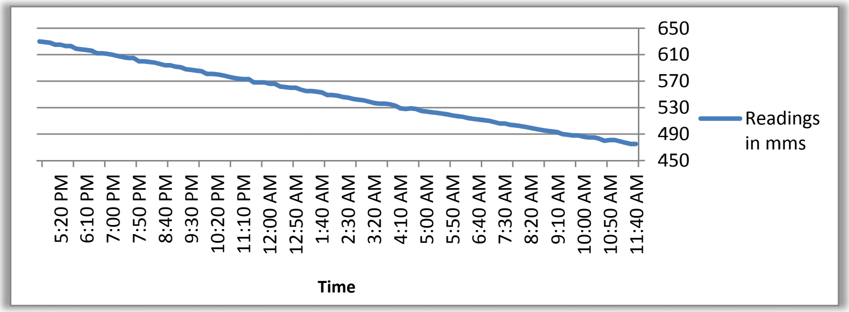


Fig. 10. Water level measurements from stilling well at a test site with a small controlled leakage for 19 hours

4 Stilling Well and Civil Infrastructure

To protect WSN against harsh outdoor environment and to provide a relatively stable water surface to be read by the ultrasonic sensor we have designed the infrastructure to achieve these objectives. In hydraulic engineering this type of structure is called a stilling well (Refer Fig. 11) which necessarily consists a concrete lined box installed on either side of a channel and is hydraulically connected to the channel through a conduit. A reinforced concrete wall is composed of a square steel grid immersed in a dielectric slab (concrete). This structure offers a resonant behavior when the signal reaches the wall and, due to this phenomenon, an FSS (Frequency Selective Surface) reflector appears. FSS reflector may act as band stop filter for GSM frequencies. Thus, steel reinforcement is avoided in the civil structure. Fig. 12 shows cross section of stilling well across canal.

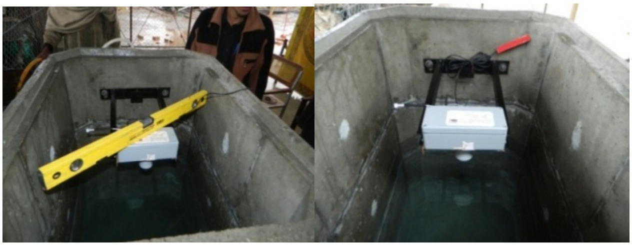


Fig. 11. Instrument installations, alignment and leveling and an Installed Unit

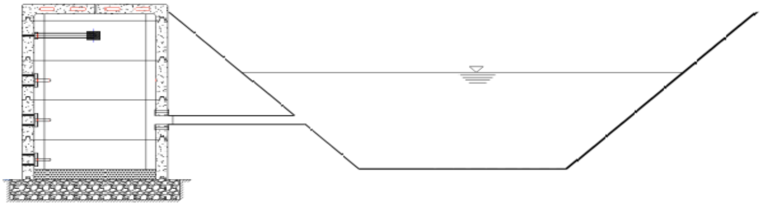


Fig. 12. Cross section of stilling well across canal

While designing the stilling well, we considered several important matters. Pre-cast segments were used in construction to achieve uniformity and cost effectiveness. The stilling well is wide enough that it could not interfere with the cone of ultrasonic signal and to enable personal access to its base for annual cleaning. An arrangement has been made for leveling the WSN; with nuts on the side wall we can align the instrument properly. WSN is installed on a metal frame. The stilling well is assembled strong enough to bear the harsh outdoor environment; therefore it is constructed of high strength PCC concrete. The structure is constructed in segments of 1 foot to facilitate handling and transportation. The segments are joined together with high strength 2-part thixotropic epoxy adhesive to eliminate seepage and to provide significant strength while in tension from lateral force.

5 Conclusion

A low-power water discharge measurement has been developed which is suitable, affordable and ready for wide-scale deployments in irrigation canal networks of the Indus river basin. GSM/GPRS based transmission is chosen as a suitable technology for communication whereas ultrasound based ranging is found suitable for sensing water levels. Power requirements, packaging, installation and system integration issues have been addressed and resolved.

References

1. Afzal, M.: Managing water resources for environmentally sustainable irrigated agriculture in Pakistan. Pakistan Development Review 35, 977–988 (1996)
2. Bandaragoda, D.J., Saeed ur Rehman, S.: Warabandi in Pakistan's canal irrigation systems: Widening gap between theory and practice. IWMI (1995)
3. Briscoe, J., Qamar, U.: Pakistan's Water Economy Running Dry. Oxford Univ. Pr. (2009)
4. Cantoni, M., Weyer, E., Li, Y., Ooi, S., Mareels, I., Ryan, M.: Control of large-scale irrigation networks. Proceedings of the IEEE 95(1), 75–91 (2007)
5. EEMB; ER34615M. Lithium Thionyl Chloride Battery (2012), `http://eemb.com`
6. Latif, M., Saleem Pomee, M.: Impacts of institutional reforms on irrigated agriculture in Pakistan. Irrigation and Drainage Systems 17(3), 195–212 (2003)
7. Lee, E.: Cyber physical systems: Design challenges. In: 2008 11th IEEE International Symposium on Object Oriented Real-Time Distributed Computing (ISORC), pp. 363–369 (2008)
8. Maxbotix; MB7380 Outdoor Ultrasonic Range Finders (2012), `http://www.maxbotix.com`
9. Nasir, H., Muhammad, A.: Feedback Control of Very-Large Scale Irrigation Networks: A CPS Approach in a Developing-World Setting. In: 18th World Congress of International Federation of Automatic Control (IFAC), Milano, Italy (2011)
10. ON Semiconductor; SMF05C Transient Voltage Suppressors (2005), `http://onsemi.com`
11. Rajkumar, R., Lee, I., Sha, L., Stankovic, J.: Cyber-physical systems: the next computing revolution. In: Proceedings of the 47th Design Automation Conference, pp. 731–736. ACM (2010)

12. Seckler, D., Barker, R., Amarasinghe, U.: Water scarcity in the twenty-first century. International Journal of Water Resources Development 15(1), 29–42 (1999)
13. SIMCOM; SIM900D GSM/GPRS Module Hardware Design Manual V1.03 (2010), `http://www.sim.com`
14. Tariq, M.U., Nasir, H., Muhammad, A., Wolf, M.: Model-Driven Performance Analysis of Large Scale Irrigation Networks. In: IEEE/ACM International Conference on Cyber-Physical Systems (ICCPS), Beijing, China (2012)
15. Wolf, W.: Cyber-Physical Systems. Computer 42(3), 88–89 (2009)

Communication Technology That Suits IoT – A Critical Review

Aqeel-ur-Rehman[1,*], Kashif Mehmood[2,**], and Ahmed Baksh[2,**]

[1] Faculty of Engineering Sciences and Technology,
Hamdard University, Karachi, Pakistan
aqeel.rehman@hamdard.edu
[2] GSESIT, Faculty of Engineering Sciences and Technology,
Hamdard University, Karachi, Pakistan

Abstract. Communication technologies play an important role in any wireless network. The networks comprise on energy constraint devices require low power communication technologies. Internet of Things (IoT) is a new and progressing concept that provides connectivity to the Internet via smart sensing devices to attain identification and management in a heterogeneous connectivity environment. Various communication technologies for Wireless Personal Area Networks (WPAN) like IoT are available presenting several properties. IoT concept involves all heterogeneous objects around us communicating with each other locally and via internet globally. Such kind of network poses several challenges and requirements for choosing the best amongst the available communication technologies. This paper is intended to present a critical study of IoT requirement, issues and challenges and propose the best or suitable amongst the available communication technologies.

Keywords: Internet of Things, Communication technologies, Wireless Sensor Network, Smart Devices, Wireless Personal Area Network.

1 Introduction

Many connected devices are approaching the new communication technologies due to their networks and services approaches as per their limits and available resources. The new communication technologies have a provision to provide seamless connectivity which is the requirement of IoT. Communication technologies used in IoT has low power consumption, low bandwidth used, low computation power, seamless communication with devices in environment due to the concept of IoT is computing for everyone, anywhere, any network and any service. Moreover, these technologies are very much penetrating in e-health, e-traffic management, e-disaster management etc.

[*] Associate Professor.
[**] MS Student.

F.K. Shaikh et al. (Eds.): WSN4DC 2013, CCIS 366, pp. 14–25, 2013.

Internet of Things is one of the important new concepts that provides connectivity of sensors and devices to the internet that provides connectivity to everyone, anywhere and anytime. The application of IoT towards home appliance, vehicles and environment demands the availability of Smart objects that are capable to sense other objects and able to communicate and interact with each other without the intervention or involvement of humans.

In this paper, the importance of IoT in terms of different communication technologies has been discussed that will make IoT suitable for different applications in terms of its various challenges and requirements.

2 The Vision of IoT

The Internet of Things (IoT) term was first coined by Kevin Ashton in 1991 [1]. As the technology and implementation ideas are moving forward, the definition of term is evolving [2]. There are two vision of IoT (i) Things Oriented vision and (ii) Internet Oriented vision [3]. The first vision involves RFID as a simple thing to be the part of Auto-ID Lab while the second vision was based on network as core technology leading to Semantic Web. The definitions above covered the way to the ITU vision of IoT, according to which: “from anytime, anyplace connectivity for anyone, we will now have connectivity for anything”.

After computer, Internet and mobile communication networks, IoT is a new wave in Information world. Internet of Things affirms to a huge network involving Internet and multiple sensor equipments to collect information [4-6]. The purpose to build such network is to recognize, locate, track, administer, and trigger the relative events.

3 IoT Architecture

IoT architecture is of three layered architecture (refer to Fig. 1). The functionalities of the layers are specified below:

Perception Layer. Object identification and information collection is the main function of this layer. It comprises of sensors, actuators, RFID tags, RFID readers/ writers and information display units (like PDA, Tablet PC, cell phone etc.)

Network Layer. Information transfer that is collected via perception layer is the main objective of this layer. Wireless Networks, wired networks, Internet, network management systems are the major components of the network layer.

Application Layer. Event detection, intelligent solutions and to perform user required functions is the responsibility of this layer.

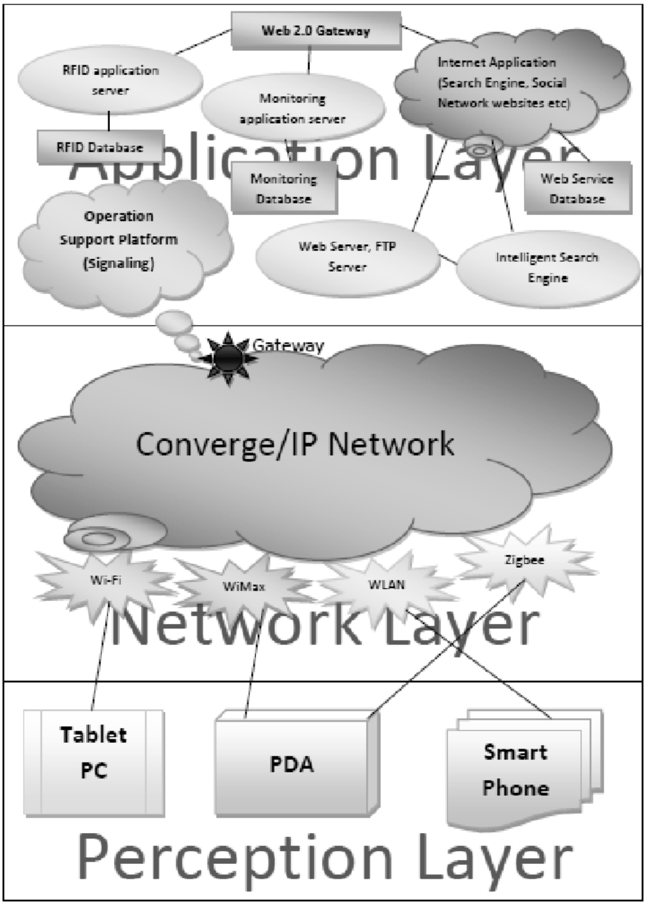


Fig. 1. Internet of Things (IoT) Architecture

4 Challenges

There are many challenges that are linked with the IoT highlighted below:

Standards. There is no standard available for the deployment of IoT globally that may make it conventional for the people [7].

Network Foundation. Limitations imposed due to the current Internet architecture for mobility, scalability, manageability and availability, IoT network establishment is facing difficulties [8].

Security, Privacy and Trust. The crucial areas in IoT are Security, Privacy and Trust. In Security area, IoT domain is facing the following challenges [8-9]:

- Security to be ensured at design time and execution time for the architecture of IoT
- Proactive identification and protection of IoT from arbitrary attacks (e.g. DoS and DDoS attacks) and malicious software.

Privacy is the second major concern. The main challenge in acceptance of IoT globally is the privacy of quantity of connected objects. The term of privacy in IoT means user/ object privacy that is facing specific challenges that are:

- There is no privacy control over personal information and location privacy of individual's physical location and movement.
- Unavailability of Standard Operation Procedures (SOPs)/methodologies and tools, privacy enhancement technologies and relevant protection laws.

Trust is having the specific following challenges:

- The System must provide the environment for easy and natural exchange of critical, protected and sensitive data e.g. smart objects may communicate with the available trusted services on behalf of users /organizations.
- The IoT System design must provide built-in trust facility for each available service.

Managing Heterogeneity. Must be able to overcome applications, environments and devices heterogeneity. The management of heterogeneity posses the major challenges that are [8]:

- Need of useful services for managing large amount of data
- Required affective mechanisms for sensor data discovery, senor data querying, publishing and subscribing; and design architecture for sensor data communication protocols, sensor networking and storage.
- Need appropriate mechanisms for sensor data stream processing, data mining, correlation, and aggregation filtering techniques. For this reason, regulate heterogeneous technologies, devices etc.

Identification and Authentication. In IoT, purpose of identification and tracking entities is to protect identification from tracking by unauthorized attacks in the network. It must be provided to users with right control over the privacy of their personal information [3].

Trust and Ownership. The trust and ownership is most currently discussing issue that how we trust on the information captured and communicate with the global network securely and reliably? Trust involves the authority and integrity of the communicating parities, accurate sensing of the data, and legal reader partnership [10].

Integration and Coordination. The challenge in IoT is how to collaborate with two different type of network, one of them is internet and other is the physical world and they work as a joint venture for meaningful results. In the integration, the major issues are cost, stability, communication speed, bandwidth, trust and security of the physical world and the internet [7]. IoT requires collaboration and teamwork among people, programs, process and services to globally share the data [11].

Regulation. The Regulation means that the processes work under IoT with settled rules. There are three different regulations (i) traditional government, (ii) international agreements and (iii) self-regulations. The Traditional government regulation is being limited in its domain and do not suit the global structure of IoT. On the other hand, self-regulation is cost effective and well-organized but only few interest and righteous thing may take part in it. For international agreements an international body such as WTO may work as legislator [12].

5 Communication Technologies in IoT

The major communication technologies that can be utilized by IoT devices are summarized below:

5.1 ZigBee

ZigBee is IEEE 802.15.4 standard. It is reliable wireless networking technology which developed by ZigBee Alliance. It is designed for limited range network monitoring and controlling due to its low data rate and short range. The main area of utilization of this technology is in Home Automation, Smart Energy devices, lighting, HVAC and security etc. Due to its low-power, high level communication protocol using small digital radios, it comes under wireless personal area network (WPAN). It also has a unique functionality of self-organizing, multi-hop and reliable mesh networking with long battery life time [13-15].

5.2 RF Links

Another preference to connect devices and make them talk is utilize simple radio frequency (RF) boundaries. It can provide communication range between 100m and 1km (depending on the transmission power and the antenna used).

RF communication modules do not provide any implementation of the TCP/IP communication protocol (or any other protocol). Data rates are quite low (up to 1Mpbs) and also need an Internet-enabled gateway that will provide access to the devices for making a complete IoT network.

The Radio Frequency Identification (RFID) technology has been initially introduced for identifying and tracking objects with the help of small electronic chips, called tags. RFID has been originally categorized as the enabling communication power for the Internet of Things, due to its low cost, high mobility and efficiency in identifying devices and objects. Despite RFID is very common for device identification and some information exchange [4].

Drawback. It cannot alone support the creation of IoT networks since it cannot provide any direct or indirect (e.g., through a gateway) communication to the Internet. The device proximity is also another drawback [4].

5.3 Bluetooth

Bluetooth is an IEEE 802.15.1 standard for low cost, short range and cheap devices of wireless radio technology. Bluetooth has been one of the first wireless communication protocols designed with lower power consumption for replacing short-range wired communications (in computer peripherals, mobile phone accessories, etc.), short distance data sharing and devices' mobility support. It has an exceptional property of creating personal area network during communication and discovers and communicates to its neighbor without need to be in visual line of sight. Due to its global standard it is also known as WPAN (Wireless Personal Area Network).

It is very important for the case of IoT since many of the devices that one would like to interconnect to the IoT (sensors, actuators, etc.) having limited power resources.

Drawback. A major drawback of Bluetooth is that it cannot provide direct connectivity to the Internet. Once has to provide an intermediate node, e.g., a PC that will act as a gateway to the outer world [13-14].

5.4 Bluetooth 4.0 LE

Traditionally, Bluetooth is used in a connection-oriented manner and it cannot directly connect to the internet. Once it is connected; a link is maintained even there is no data flow. The new Bluetooth low energy (BLE), old name is WiBree, is a subset to Bluetooth v 4.0. It has new protocol stack and new profile architecture. This version has been adopted as of June 2010. It provides new adverting mechanism, quick discovery and enable connection and uses Asynchronous connection-less MAC for low latency rate and fast communication. Bluetooth 4.0 is users friendly as it introduces New Generic Attribute Profile which is simpler to use [16].

5.5 6LoWPAN

The 6LoWPAN is Wireless PAN with low power and supports IPv6 network. It is a connection oriented technology in which router forward the data to its next hop to the 6LoWPAN gateway which is connected to 6LoWPAN with the IPv6 domain and then forward the data to its respected device correctly.

With IPv6 we have enough address space to identify all the things in the world. In IP based network standard protocols (HTTP, TCP/IP) are directly applied on sensor nodes just as they do with traditional web servers out there in the Internet [11][17].

5.6 Z-Wave

Z-Wave protocol architecture developed by ZenSys and promoted by the Z-Wave Alliance. It is another low power consuming which mostly used in automation and light commercial environment. It has an open communication protocol. The main purpose of Z-wave is for a reliable massage passing from a control unit to one or more nodes in the network. Z-wave have two types of devices, one is poll Controllers which send commands to the slaves, the second type of device, which reply to the controller to execute the commands [6][18].

5.7 WiFi

Wireless fidelity is known as Wi-Fi, the IEEE 802.11x standards, is the most common way to connect devices wirelessly to the Internet. Laptop, Smartphone and Tablet PC are equipped with WiFi interfaces and talk to wireless router and provide two way accesses to the Internet. The Wi-Fi standard family allows establishing wireless network on short distances. Wi-Fi has series types of networks like IEEE 802.11, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11e: QoS extension, IEEE 802.11f: extension for managing handover and IEEE 802.11i security extension. The Wi-Fi group is working on unlicensed spectrum of 2.4 GHz (ISM) band.

Table 1. Communication Technologies – A Comparision

Standard	**Bluetooth**	**Bluetooth 4.0 LE**	**ZigBee**	**Wi-Fi**	**6LoWPAN**	**RF – Link**	**Z-Wave**
IEEE Spec.	IEEE 802.15.1	IEEE 802.15.4	IEEE 802.15.4	IEEE 802.11a/b/g/n	IEEE 802.15.4 2006	IEEE C95.1 –2005	Z-Wave alliance
Topology	Star	Star	Mesh, Star, Tree	Star	Mesh, Star	-	Mesh
Bandwidth	1 Mbps	1 Mbps	250 Kpbs	Upto 54 Mbps	250 Kbps	18 MHz	900 MHz
Power Consumption	Very Low	Very Low	Very Low	Low	Very Low	Very Low	Very low
Max. data rate (M bit/s)	0.72	1	0.25	54	0.25	1	9600 bits or 40 kbits
Bit time (μs)	1.39	-	4	0.0185	-	-	-
Range	<30 m	5-10 m	10-300 m	4-20 m	800 m (Sub-GHz)	<3 m	30 m
Spectrum	2.4 GHz	2.4 GHz	2.4 GHz	2.4-5 GHz	2.4 GHz	2.4 GHz	2.4 Ghz
Channel Bandwidth	1 MHz	2400 – 2480 MHz	0.3/0.6 MHz, 2 MHz	22 MHz	868 – 868.6 MHz (EU) 902-928 MHz (NA) 2400 – 2483.5 MHz (WW)	-	868 MHz

The 802.11e standard will include two operating mode for improving the services of voice (i) Wi-Fi Multimedia Extensions (WME) – Mandatory and (ii) Wi-Fi Scheduled Multimedia (WSM) – Optional.

The commercially available WiFi modules (like the one WiFi communication module in a pluggable form known as XBee series modules) can be directly integrated to an IoT device and provide instant connectivity. The major advantage over the other wireless technologies is the fact that WiFi networks are very easy to establish and thus IoT devices with WiFi modules can have direct connection to the Internet.

Drawback. This technology (which was at no means designed for IoT networks) is more power demanding than the others [14-15].

6 Requirements of IoT

In IoT, heterogeneous devices and communication technologies are used to develop a seamless computing for everywhere. In this regard, we must need improvement in energy, communication, resource constrained, scalability, modularity, extensibility and interoperability among heterogeneous things and their environments that are the key design requirements for IoT [10].

6.1 Energy

Energy problems, in all its phases, from gathering to conservation and usage, are central to the development of the IoT. There is a need to research and grow solutions in this area (nano-electronics, semiconductor, sensor technology, micro systems integration) having as an objective of ultra low power devices, as existing devices seem insufficient considering the processing power needed and energy restrictions of the future.

6.2 Intelligence

Abilities such as self-awareness, context awareness and inter-machine communication are well-thought-out a high priority for the IoT. Mixing of memory and processing power and the ability to endure harsh environments are also a high priority, as are the best possible security techniques. Novel cognitive approaches that leverage opportunistically on the time dependent available heterogeneous network resources can be accepted to support unified continuous access to the information network as well as grip irregular network connectivity in harsh and/or mobile environments. “Intelligent” methods to knowledge discovery and device control will also be important research challenges.

6.3 Communication

New smart antennas (fractal antennas, adaptive antennas, receptive directional antennas, plasma antennas) that can be fixed in the objects and made of new materials are the communication means that will permit new advanced communications systems on chip. Modulation schemes, transmission rates, and transmission speed are also major issues to be undertaken. New advanced solutions need to be defined to efficiently support mobility of billions of smart things, possibly well-found with multiple heterogeneous network resources. Last but not least, network virtualization techniques are key to confirm an evolutionary path for the arrangement of IoT applications with secure Quality of Service (QoS).

6.4 Integration

Integration of wireless identification technologies (like Radio Frequency Identification — RFID) into packaging, or, rather, into products themselves will allow for important cost savings, improved eco-friendliness of products and allow a new dimension of product self-awareness for the help of customers. Integration requires addressing the need for heterogeneous systems that have sensing, acting, communication, cognitive, processing and compliance features and includes sensors, actuators, nanoelectronics circuits, embedded systems, algorithms, and software embedded in things and objects.

6.5 Dependability

Dependability of IoT systems is of supreme importance; so the IoT network structure must ensure reliability security and privacy by supporting individual authentication of billions of dissimilar devices using heterogeneous communication technologies across different executive domains. Reliable energy-efficient communication protocols must also be intended to confirm dependability.

6.6 Semantic Technologies and IoT

IoT requires devices and applications that can easily connect and interchange information in an ad-hoc way with other systems. This will involve devices and services to prompt needs and capabilities in formal ways. To enable the interoperability in the IoT further research into semantic technologies is needed. Examples of challenges are large-scale dispersed ontologies, new methods to semantic web services, rule engines and methodologies for hybrid reasoning over large heterogeneous data and fact bases, semantic-based discovery of devices and semantically driven code generation for device interfaces.

6.7 Modeling and Design

The design of large-scale IoT systems is stimulating due to the large number of heterogeneous components involved and due to the complex duplications among devices introduced by cooperative and distributed approaches. To cope with this issue, original models and design frameworks need to be planned; for example, inspired by co-simulation methods for large systems of systems and hardware-in-the-loop approaches.

7 Requirement of Communication Technologies in IoT

The IoT Communication Technologies should provide a seamless communication and secure access to the internet anywhere, anytime, any network at any bandwidth/speed. We should never feel any difference to its indoor or outdoor communication. It should have unlimited range, zero latency rate and unlimited throughput. On the other hand, it should also cost effective and low energy consumption. It should also ensure the protection of privacy. Some of the requirements discussed for communication technologies in IoT are [19]:

- *Range and dissemination.* Due to walls, window, plants and etc. it is deployed in wide area, but the power consumption and throughput are inversely proportional to the range.
- *Power Consumption.* Low power operated devices for resulting low throughput and range.
- *Throughput.* Need for high throughput means the sustainable power of battery life and better coverage area.
- *Number of devices.* If the more devices used it consumes more resource and performance of computation is affected.
- *Types of network supported.* Due to variable length of topologies used like mesh, tree, peer-to-peer etc. that have their own advantages and drawbacks according to its standardization, throughput and range and other.
- *Globalization usage.* Some of the technologies are used in their boundaries (countries) due to its regulations and issues.
- *Mobility.* Must support the mobility of devices whether it is working in any location and environment.
- *Failover capabilities.* Need to be fast backup solution in case of network fails.
- *Multi-protocol support.* Must support multiple networks for its situation.
- *Security and Privacy.* All the communication is needed to be in secured manner and no unauthorized access to break the privacy of any data.

8 Discussion on IoT Communication Technologies

Following are the technologies amongst the above mentioned technologies (refer to Table 1) that suits most of the requirements of IoT:

Wi-Fi IEEE 802.11x is wireless LAN. It provides point-to-point and point-to-multi point high speed and robust communication. It allows multiple users to connect in the same time period to same frequency band with minimum interference to the other users. Wi-Fi operates on three different non-interoperable technologies i) Frequency Hopping Spread Spectrum (FHSS) ii) Direct Sequence Spread Spectrum, iii) and Infrared (IR). Wi-Fi 802.11n Technology, based on Multiple Input Multiple Output (MIMO) technology is intended to increase the data rates upto 600 Mbps and onwards. IEEE 802.11i is known as (WPA–2) that enhances the cyber security and Advanced Encryption Standard (AES) which fulfill the IoT requirement. It is easy to install, supports mobility of devices, and less expensive. The reliability and availability is achieved by applying proper path engineering and system design techniques. The proper implementation of massage acknowledgement, error correction algorithms, data buffering etc. enhances the reliability of massage transmission over wireless medium. In addition, 802.11ah (working on Wi-Fi on ISM bands below 1 GHz) modify it for ad-hoc, mesh networking, infrastructure-independent and longer-range control of sensor networks therefore, the band new-technologies better suited for certain aspects of IoT communication and be a part in future of IoT.

The low power, cost effective ZigBee is reliable for home area wireless network developed by ZigBee Alliance based on an open global standard. It works on 2.4 GHz unlicensed frequency of IEEE 802.15. 4 standard. The major achievement in ZigBee technology is long battery life cycle but it is depending upon the topology adopted. Due to its high battery life and low power consumption, it is mostly used in home automation but in industrial environments it is not well adapted.

Bluetooth is low power short range radio frequency based Wireless Personal Area Network (WPAN). It can facilitate both point-to-point and point-to-multipoint communication configuration. The advance achievement is Bluetooth 4.0 low energy consumption technology. Bluetooth Low Energy (BTLE) is being used in health care industry for portable medical and lifestyle devices. It's preventing highly influenced by surrounding communication link and may interference in IEEE 802.11 WLAN network technology. The provide security, scalability and reliability authorization techniques are used before transmit or receive any kind of information.

9 Conclusion

IoT is a new and emerging concept that gaining popularity day by day. It involves smart devices available all around us and networked them as WPAN locally while globally as Internet. Such connectivity requires wireless communication technologies like Bluetooth, Wi-Fi, ZigBee, Z-Wave and RF Link. Every concept poses it specialized requirement for optimal utilization. In this paper, we critically analyzed the issues, requirements and challenges of Internet of things (IoT) specifically related to communication technology. Critical analysis presents Bluetooth LE, 6LoWPAN and WiFi as suitable candidates for future IoT but many issues are still to address for which some new technologies are in demand.

Acknowledgement. This work is partly supported by Center of Research in Ubiquitous Computing, Hamdard University chapter from which the authors are associated.

References

1. Ashton, K.: That 'Internet of Things' Thing. RFiD Journal 22, 97–114 (2009)
2. Atzori, L., Iera, A., Morabito, G.: The internet of things: A survey. Computer Networks 54(15), 2787–2805 (2010)
3. ITU Internet Reports 2005: The Internet of Things, `http://www.itu.int/osg/spu/publications/internetofthings` (accessed on September 19, 2011)
4. International Telecommunication Union UIT. ITU Internet Reports 2005: The Internet of Things[R] (2005)

5. Gustavo, R.G., Mario, M.O., Carlos, D.K.: Early infrastructure of an Internet of Things in Spaces for Learning. In: Eighth IEEE International Conference on Advanced Learning Technologies, vol. 2, pp. 381–383 (July 2008)
6. Sarma, A.C., Girão, J.: Identities in the future internet of things. Wireless Personal Communications 49(3), 353–363 (2009)
7. CERP-IoT: Cluster of European Research Projects on the Internet of Things, Vision and Challenges of Realizing the Internet of Things (March 2010), http://www.internet-of-things-research.eu/pdf/IoT_Clusterbook_March_2010.pdf (accessed on May 2012)
8. Internet of Things Strategic Research Roadmap, http://www.grifs-project.eu/data/File/CERP-IoT%20SRA_IoT_v11.pdf (accessed on April 2012)
9. Agrawal, S., Das, M.L.: Internet of Things—A paradigm shift of future Internet applications. In: 2011 Nirma University International Conference on Engineering (NUiCONE), pp. 1–7 (December 2011)
10. Newmarch, J., Tam, P.: Issues in Ownership of Internet Objects. In: The Fifth International Conference on Electronic Commerce Reaserch, Montral, Canada (2002)
11. Petrie, C.: The Future of the Internet is Coordination. In: Proceedings of FES-2010: Future Enterprise Systems Workshop (2010)
12. Weber, R.H., Weber, R.: Internet of things: legal perspectives. Springer Publishing Company, Incorporated (2010)
13. ZigBee – The Internet of Things, http://www.vesternet.com/zigbee (accessed on November 2012)
14. Doukas, C.: Building Internet of Things with the Arduino. CreateSpace Publishers (2012)
15. Lee, J.S., Su, Y.W., Shen, C.C.: A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi. In: 33rd Annual Conference of the IEEE Industrial Electronics Society (IECON 2007), pp. 46–51 (November 2007)
16. Decuir, J.: Bluetooth 4.0: Low Energy, IEEE Annual Report (2010), http://chapters.comsoc.org/vancouver/BTLER3.pdf (accessed on October 2012)
17. Ee, G. K., Ng, C. K., Noordin, N. K., Ali, B. M.: A Review of 6LoWPAN Routing Protocols. In: Proceeding of Asia Pacific Advanced Network (2010)
18. The Danish Electricity Saving Trust's concept for energy saving devices, metering equipment and wireless communication, http://www.savingtrust.dk/publications/concepts/dests-concept-for-energy-saving-devices-metering-equipment-and-wireless-communication (accessed on December 2012)
19. Mainetti, L., Patrono, L., Vilei, A.: Evolution of wireless sensor networks towards the Internet of Things: A survey. In: Software, 19th International Conference on Telecommunications and Computer Networks (SoftCOM), pp. 1–6 (September 2011)
20. Machine-to-Machine Communications: Connecting Billions of Devices. OECD Digital Economy Papers, No. 192, OECD Publishing (2012), http://dx.doi.org/10.1787/5k9gsh2gp043-en
21. Bandyopadhyay, D., Sen, J.: Internet of Things: Applications and Challenges in Technology and Standardization. Wireless Personal Communications 58(1), 49–69 (2011)

Cooperative Vehicle-to-Vehicle Awareness Messages Implementation

Virginia de Cózar[1], Javier Poncela[1,2], Marina Aguilera[1],
Muhammad Aamir[3], and Bhawani Shankar Chowdhry[4]

[1] ETSI Telecomunicacion, University of Malaga, Spain, E-29071
virdecozar@gmail.com, jponcela@uma.es
[2] Visiting Professor, IoBM, Karachi, Pakistan
[3] Sir Syed University of Engineering & Technology, Karachi,
Pakistan and Mehran University of Engineering & Technology, Jamshoro, Pakistan
muaamir5@yahoo.com
[4] Mehran University of Engineering & Technology, Jamshoro, Pakistan
c.bhawani@ieee.org

Abstract. Wireless technologies are bringing about a new conception on transport systems. New technologies provide support for increased security, reduced congestion thus optimizing the already existing road network and better mobility support. The standard CAM (Cooperative Awareness Messages) is one of the components of the reference architecture defined by the European Telecommunication Standards Institute (ETSI) for transmitting geographically aware information with relevant date for other vehicles. This work addresses the development of a collaborative environment that demonstrates the use and effectiveness of CAM messages based on standard ETSI EN 302 665 [12].

Keywords: Intelligent Transport System, Vehicle-to-Vehicle communications, Cooperative Awareness Messages.

1 Introduction

The conceptual change required in transport systems arises from the demographic and socioeconomic transformations that will take place in this century. The growth of global population, extensive urbanization and a foreseen huge increase in the number of vehicles ([4], [9], [30]) require new ideas to make transportation secure, efficient and sustainable. Though the motor industry raises big challenges, such as improved traffic safety, traffic congestion or environmental impact, it cannot be overlooked that vehicles play an essential role in our modern society. But the high number of casualties force new solutions through the use of advanced technology in order to mitigate casualties.

New technologies provide support for increased security, reduced congestion via optimizing the already existing road network and better mobility support as actual status of the road network is known to all participants allowing for optimal route selection.

F.K. Shaikh et al. (Eds.): WSN4DC 2013, CCIS 366, pp. 26–37, 2013.

Modern cars are better equipped than mid-20th century aircraft: proximity radar, GPS, wheel sensors and actuators, etc. The so-called 'Vehicle to Vehicle' communications technology (V2V) or 'Vehicle to Infrastructure' (V2I) [26] are part of a cooperative environment that allows provision for new and innovative applications, such as help on crossroads, help for overtaking, accident information, traffic density, etc. One of the driving ideas behind this technology is that critical driving conditions can be identified and related information can be exchanged between the vehicles, for example hazardous location warning, such as ice on the road. Risks can be anticipated and appropriate measurements taken. Figure 1 shows the current Intelligent Transportation System (ITS) vision.

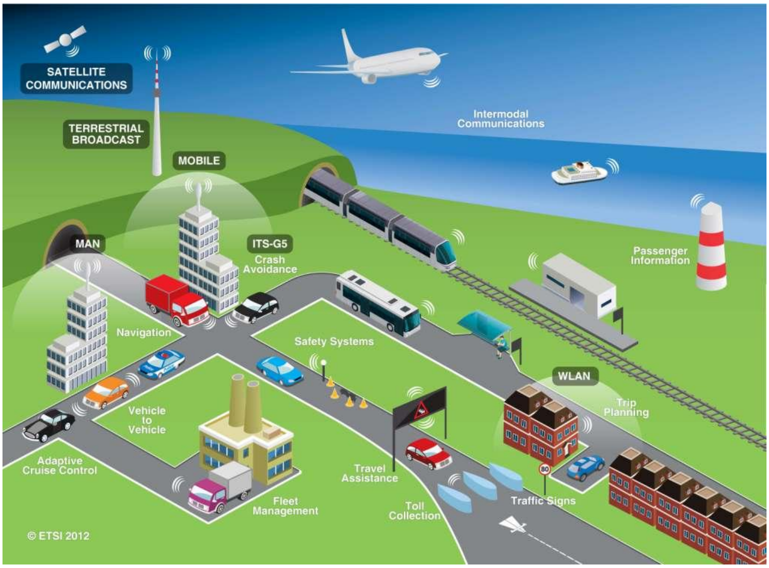


Fig. 1. Scenario for ITS systems [20]

The ad-hoc networks formed by vehicles are known as Vehicular Ad-hoc Networks (VANETs) [22], which are a particular type of MANETs (Mobile Ad hoc Networks) but with special characteristics and constraints. The highly dynamic topology and the non uniform distribution of the nodes represent a great challenge for the networking strategies. Due to the high mobility of the nodes, standard MANET protocols are not appropriate for transferring information in this kind of networks. Routing protocols that exploit geographical information look very promising.

The standard CAM (Cooperative Awareness Messages) [16] is one of the components of the reference architecture defined by the European Telecommunication Standards Institute (ETSI) for transmitting geographically aware information with relevant data for other vehicles. The aim of this work is the design and implementation of a cooperative framework based on CAM.

This paper is organized as follows. The next section presents a brief description of the state of the art on this area. Section 3 describes mechanisms for geographical routing. Section 4 describe the CAM module implementation. Section 5 is the conclusion.

2 State of the Art

The term Intelligent Transport Systems refers to a wide range of information technologies applied to the transport sector. Though it might seem surprising, ITS technologies are not a novelty. The automotive sector has been working for a long time to incorporate technologies for the safety of drivers and passengers. Some of these advances have been ABS (Antilock Brake System) or assisted direction. Also, the introduction of the CAN (Controller Area Network) [25] protocol was a significant milestone. However, the wireless technologies, detection and navigation systems, and so on, have originated a new view on the security and efficiency on the transport sector, leaned towards the cooperation between vehicles and their surroundings.

The use of ICT technologies has opened the door to many varied applications that previously where vetoed. The new security applications focus on guaranteeing, preventing and increasing security during the journey, for example, applications as eCall [17], where an emergency call is launched when an accident happens, automatically providing location information so that emergency response times are lower. Efficiency is improved through traffic optimization mechanisms, via control centres that may organise traffic and resources in real-time. Value-added applications, such as infotainment (information-entertainment), will make journeys more pleasant. The full set of envisioned applications will certainly need of the cooperation among users (vehicles) and with the road infrastructure.

Wireless technologies have brought a revolutionary change in ITS systems, transforming vehicles into highly complex communication stations. Depending on the target application, they will use short-range communications, such as NFC (Near Field Communication), Bluetooth o CEN DSRC (Dedicated Short Range Communication), being the latter the one used for motorway payments; cellular technologies such as WiMAX, GSM/UMTS and, in the future, LTE (Long Term Evolution); or even broadcast services, such as GPS (Global Positioning System), DAB/DVB-T (Digital Audio/Video Broadcasting).

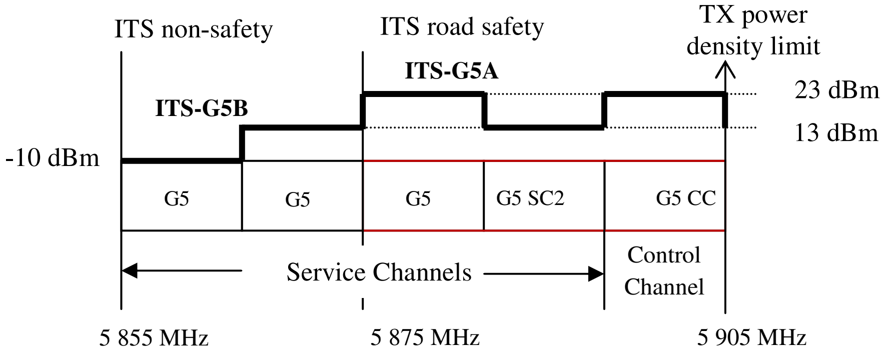


Fig. 2. Frequency bands for ITS-G5 en EU

The real drivers for this new scenario have been the security applications. As such, communication technologies must provide for high reliability, low latency and support for cooperative ad-hoc environments. None of the previously mentioned technologies do really meet these requirements, which led to the development of a new technology based on IEEE 802.11, the IEEE 802.11p standard. The bandwidth allocated for it was band 5875-5905 MHz. The ETSI standard [13] has been based on this technology in the 5 GHz band. This profile mandates that security applications used band ITS-G5A (5875-5905 MHz) and non-security applications use band ITS-G5B (5855-5875 MHz) (see Figure 2).

It is worth mentioning European R&D project funded by the European Commission such as COMeSafety [5], CVIS [7], Safespot [8], Coopers [6], PreDrive C2X [27] or GeoNet [18]. Besides, there are several other initiatives such as Intelligent Car which aim to promote the deployment of ITS systems. Also, an industrial consortium has been created, Car-to-Car Consortium (C2C-CC) [3], with the goal of increasing security and efficiency in vehicular environments through the use of ITS systems. ETSI, through its Technical Committee ITS, carries out the standardization process for road transport. Table 1 shows some of the standards and technical reports.

Table 1. ETSI technical documents for ITS

Name	Standard
Basic Set of Application	[TR 102 638]
CAM	[TS 102 637-2]
DENM	[TS 102 637-3]
ITS Communication Architecture	[EN 302 665]
Network Architecture	[TS 102 636-3]
BTP	[TS 102 636-5-1]
GeoNetworking SubPart 1: Media-Independent Functionality	[TS 102 636-4-1]
GeoNetworking SubPart 1: Media-Dependent Functionality	[TS 102 636-4-2]
Ipv6 over GeoNetworking	[TS 102 636-6-1]
European Profile in 5 GHz (ITS-G5)	[EN 202 663]

From the communications point of view, an ITS station [1], has a protocol stack organized in four layers (the reference network architecture is shown in Figure 3): Access layer, Networking & Transport layer, Facilities layer and Applications layer. Besides, there are two more vertical cross-layers: Management layer and Security layer. The Networking & Transport layer supports both common IP protocols together with ITS specific ones.

One of the innovative characteristics of ITS is the use of geographical routing. The GeoNetworking protocol ([14], [23]) allows a station to not only provide point-to-point or point-to-multipoint routing but also provide information for stations located in a given geographical area (Figure 4). This type of routing is based on two main assumptions: a) Every node is aware of its own position since this information is provided by a positioning device, such as a GPS; and, b) every node knows the position of its one-hop neighbours because all nodes are exchanging beacons periodically. A beacon carries at least the node identifier and its current movement information (position, speed and heading). Position-based protocols are divided in two approaches: Unicast-based geographical routing protocols and broadcast-based geographical routing protocols. The optimal communication mode is different for each application.

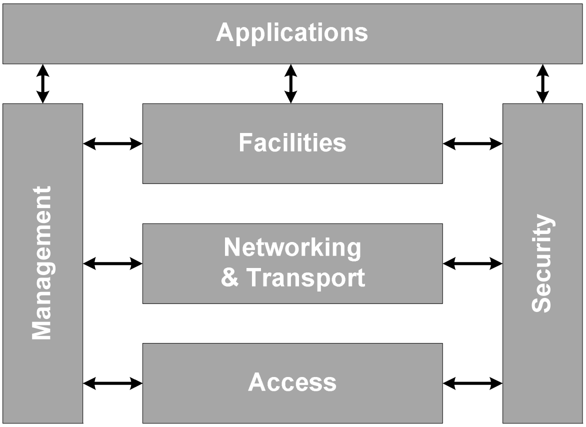


Fig. 3. Reference architecture for an ITS stations

Different types of messages have been defined to be exchanged in the network layer. Each message reports a different type of information and has its specific network layer requirements. The COMeSAFETY [5] project defines message types like Cooperative Awareness Message (CAM), Decentralized Environmental Notification Message (DENM), Event Message (EM), Periodic Message (PM) and Service Messages (SM).

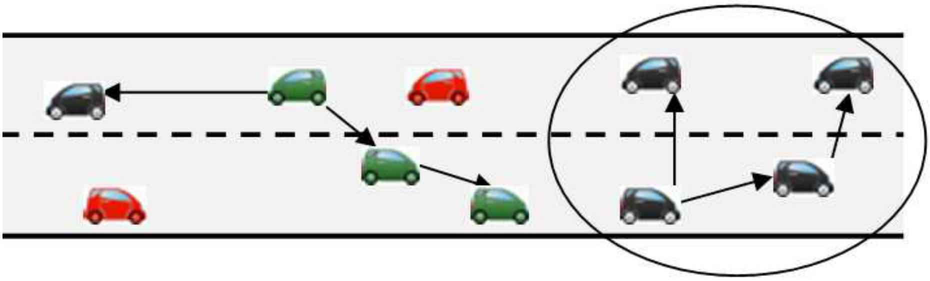


Fig. 4. GeoNetworking protocol scenario

The CAM protocol [16] is part of the Facilities layer. CAM messages are periodically sent and contain basic safety relevant status information like node actual position, speed, acceleration or heading as well as the node identifier. Each station of the network has to send these messages with a frequency comprised between 0.5 and 2 Hz independently of the applications installed on the nodes. The communication method is single-hop broadcast because this information is only relevant in the vicinity. The time validity of the information is also short due to the dynamic condition of this information. Therefore, there are no network layer requirements for these messages because they do not need to be distributed in the network. The main applications are warnings such as emergency vehicle, slow vehicle, motorcycles approaching, etc ([28], [29], [11], [24]). CAM has defined four profiles depending on the type of ITS station: Vehicle, Infrastructure, Emergency Vehicle and Public Transport. Additional information depending on the profile type can be included in CAM messages, such as siren status for emergency vehicles.

DENM messages [19], however, are used to inform other traffic participants of special events and road conditions which can mean a danger for drivers, like roadwork construction or an accident. As they report the information related with the events they are sent only on event detection and periodically updated if the node detects the persistence of the situation for a long time. Consequently, the information in these messages may have a long term and a longer range relevancy.

3 Geographical Routing Module

The Networking & Transport layer implements a Geo-Opportunistic routing [23]. Geographic routing tries to greedily forward a packet to the furthest neighboring node that is closest toward the packet's destination [1]. The problem is that the further the distance, the higher the attenuation, and the higher the likelihood of packet loss. Solutions to this problem make use of the concept of opportunistic routing ([2], [10]) where a sender takes advantage of random packet receptions in its neighboring nodes due to the error prone wireless channel and of opportunistic forwarding by a subset of the neighbours that have received the packet correctly. The key challenge in this approach is selecting an appropriate subset of neighbours that can provide the best path toward the destination.

Every node has a register of the information of its one-hop neighbours. When the node receives a packet, it transfers the header information to the Neighbourhood Table, which, for each remote node, stores its identification, position (latitude, longitude and altitude), speed, heading and the message timestamp. This table is indexed by the node ID. The table is periodically updated and the entries older than a certain time are deleted, as their information is considered non-reliable.

There are several proposed variants for a geographical-based routing. The performance of each of these variants is greatly influenced by the actual node mobility.

The Geo-Distance routing is the most simple alternative; it is basically a Distance-based routing. In this variant, the routing layer only decides whether the packet will be rebroadcast or not. The decision is made by obtaining a random value from a uniform variable between 0 and 1 and comparing this value with a set threshold.

The Geo-Probabilistic broadcast routing adds a distance to the forwarding decision. If the random value is above the threshold and the distance from the source is also higher than a certain amount then the packet is forwarded. The purpose of this modification is to optimize the dissemination of data, decreasing the number of transmissions when the network is highly congested.

One further variation is the so-called Geo-Density routing, where the threshold values are dynamically evaluated based on the local density conditions. This value is estimated in each node from the current number of entries in its routing table.

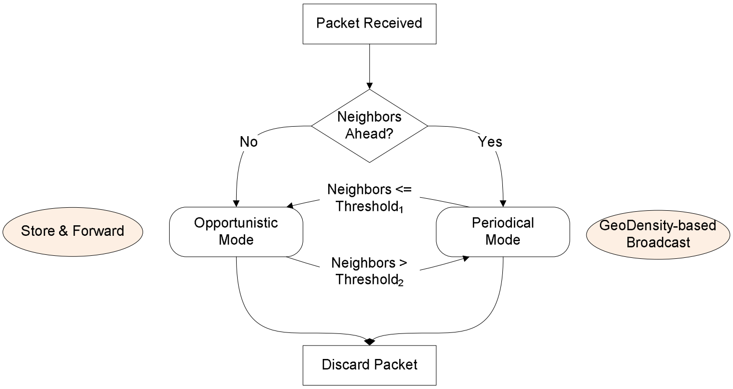


Fig. 5. Geo-Opportunistic broadcast state machine

In our system we have used a Geo-Opportunistic routing mechanism. With this approach, nodes switch between two modes depending on their current number of neighbors (Figure 5): a) nodes broadcast it repeatedly following a contention process or b) they wait and forward the message once a new node appears. The first mode is appropriate for dense traffic scenarios whereas the second one is appropriate for sparse traffic ones.

The results presented in [1] show that, for highway scenarios, this routing variant realizes the delivery of the notification messages to nodes approaching the event while avoiding an increase in the number of unnecessary retransmissions. Also, if the network is dense enough it is able to limit the message propagation geographically. The message dissemination is thus concentrated in those areas where it is more relevant.

When in the first mode, periodical broadcast, as a new notification message is received it is retransmitted with a certain probability, as was done in the Geo-Density routing. However, this procedure does not happen only once, otherwise the chance of message lost would be high. Therefore, one of the receivers will rebroadcast the message again after some time. The decision of who will rebroadcast the message is based on a contention process.

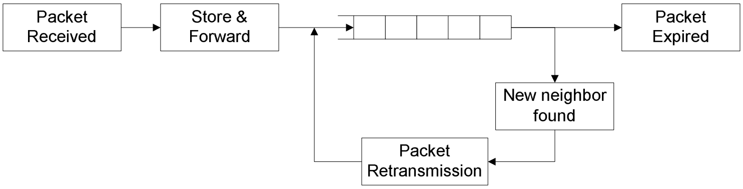


Fig. 6. Store and forward strategy

Consider now a vehicle driving on the road that receives a event notification within a its range of interest. There may occur several situations. The vehicle is driving in a populated area; in this case, it will just forward the packet to nearby neighbors. However, it may happen that there are no near vehicles that can receive the event notification forwarding. Then, the vehicle would use a store and forward strategy, thus effectively storing the packet for further retransmission when another node is available. In this strategy, nodes are grouped in clusters, and retransmission between clusters is only performed by border nodes. Only the leading node of a cluster may enter the store and forward mode; the leading node is determined by counting the number of nodes ahead. The lifetime of the packets stored in the buffer is periodically checked and outdated ones are removed (see Figure 6).

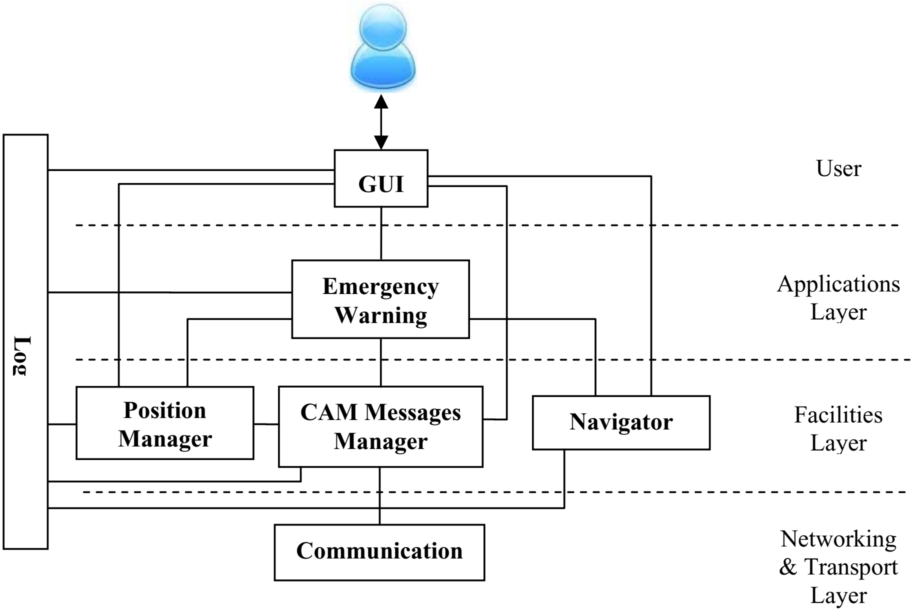


Fig. 7. Architecture of the ITS cooperative environment

4 Cooperative Module Design

The architecture of the implementation is shown in Figure 7. As it can be seen, the Applications layer contains the Emergency Warning application, which handles received CAM messages. The Facilities layer includes a CAM Message Manager, responsible for generating, coding, transmitting, decoding and receiving CAM messages, a Position Manager, which loads the current station location from a GPS receiver, and a Navigator module, for visualizing the position of nearby stations overlaid in a map. The Networking &Transport layer is responsible for reception and transmission of the actual CAM messages. In addition, two other modules are incorporated: a Graphical User Interface, for user interaction, and a Logging module, for debugging and post-analysis purposes.

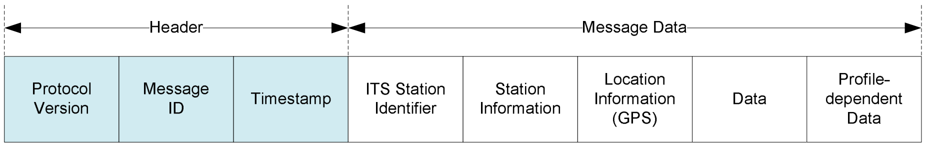


Fig. 8. Format of CAM messages

The CAM Message Manager is the core of the system. It is composed by three blocks:

(a) Message Processing module: Inserts data and codes outgoing messages, while decoding and extracting information for incoming messages. It also handles profile specific information.
(b) Transmission module: Handles message transmission. It runs as an independent background thread.
(c) Reception module: Handles message reception. As the transmission module, it is also an independent background thread.

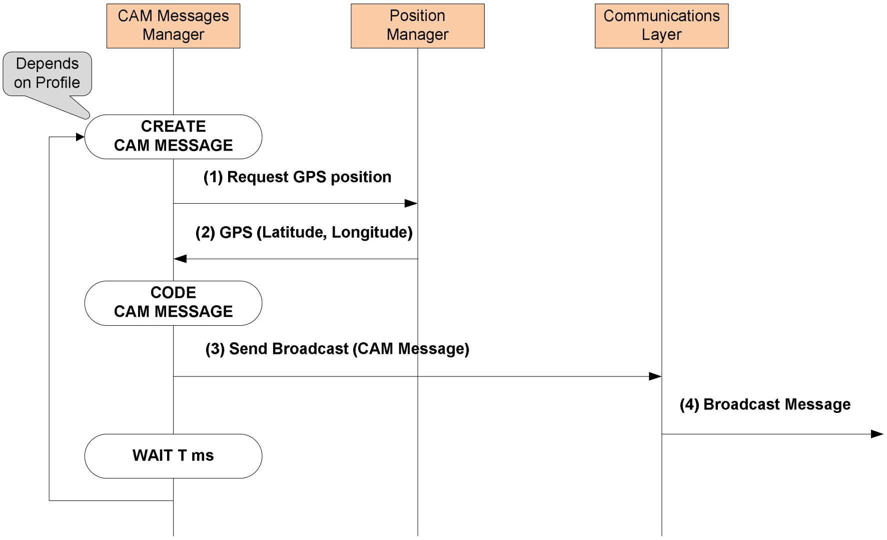
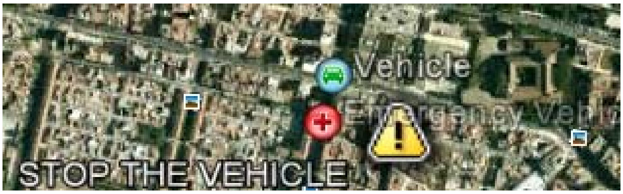


Fig. 9. Transmission of CAM messages

The format of CAM messages is given in Figure 8 [16]. Each message has a header with fields for the protocol version, the message identifier and a timestamp. The payload contains the station identifier, information about the station (i.e., if it is a mobile station, a public station, …), GPS location information, general information (speed, dimensions, switched on lights, …), profile specific data. Messages are coded using Unaligned Packet Encoding Rules (UPER) [21]. As the standard requires, messages are periodically transmitted (every 500 ms).

When a message is received, its information is extracted and passed to the Navigator module, which displays appropriate visual information for the user. In case the message proceeds from an emergency vehicle, it is passed to the Emergency Warning application, which assesses the risk and plays an appropriate warning for the user. On outgoing messages, it will obtain the location from the Position Manager and insert it in the message before it is coded. The transmission process is shown in Figure 9. Routing of these messages is performed through GeoNetworking and BTP, using band ITS-G5A.



Vehicle	🚗
Emergency vehicle	➕
Warning	⚠

Fig. 10. Example of warning display

The implementation has been demonstrated with an Emergency Warning application. This application warns of incoming emergency vehicles, with indication on which side is the vehicle approaching, and shows a risk sign when the emergency vehicle is less than 75 meters far. The Navigator module displays a map with the position of the emergency vehicle overlaid on it. The map visualization is obtained from Google Earth. Figure 10 shows the navigation display, with indication of an event (yellow sign) and one nearby emergency vehicle (red sign).

5 Conclusion

The architecture of the cooperative framework described in this paper has been based on the reference architecture of ITS stations. This work has focused on the implementation of a Cooperative Awareness Messages module as specified in ETSI standards. This module is responsible for the generation, coding, and transmission of messages between ITS stations, vehicle-to-vehicle, and may serve different user applications. One of the use cases included in the standards, the Emergency Warning application, which raises warnings to the user whenever an emergency vehicle is nearby, has been used to validate the development,

Acknowledgments. This work has been partially funded by Spanish Junta de Andalucia under project TIC-6897.

References

1. Aguilera, M., Rockl, M., Kloiber, B., de Ponte Muller, F., Strang, T.: Information-centric opportunistic data dissemination in Vehicular Ad Hoc Networks. In: 13th International IEEE Conference on Intelligent Transportation Systems (ITSC), pp. 1072–1078 (2010)

2. Biswas, S., Morris, R.: ExOR: Opportunistic Multi-Hop Routing for Wireless Networks. SIGCOMM CCR 35(4), 133–144 (2005)
3. Car 2 Car Communication Consortium (2011), http://www.car-to-car.org/
4. Cervero, R.: Growing Smart by Linking Transportation and Urban Development. Built Environment 29(1), 66–78 (2003)
5. ComeSafety: Communication for eSafety (2012), http://www.comesafety.org/
6. Cooperative Systems for Intelligent Road Safety, Coopers (2012), http://www.coopers-ip.eu/
7. Cooperative Vehicle Information Systems, CVIS (2011), http://www.cvisproject.org/
8. Cooperative Vehicles and Safe Infrastructure for road safety, SafeSpot (2013), http://www.safespot-eu.org/
9. Dicken, P., Öberg, S.: The Global Context - Europe in a World of Dynamic Economic and Population Change. European Urban and Regional Studies 3(2), 101–120 (1996)
10. Dubois-Ferriere, H., Grossglauser, M., Vetterli, M.: Least-Cost Opportunistic Routing. In: Allerton 2007, Urbana, IL (September 2007)
11. Eckhoff, D., Sommer, C., German, R., Dressler, F.: Cooperative Awareness at Low Vehicle Densities: How Parked Cars Can Help See through Buildings. In: Global Telecommunications Conference (GLOBECOM 2011), pp. 1–6 (2011)
12. ETSI EN 302 665 V1.1.1, Intelligent Transport Systems (ITS); Communications Architecture. European Standard (Telecommunications Series) (September 2010)
13. ETSI ES 202 663 V1.1.0 Intelligent Transport Systems (ITS); European profile standard for the physical and medium access control layer of Intelligent Trans-port Systems operating in the 5 GHz frequency ban. ETSI Standard (November 2009)
14. ETSI TS 102 636-1 V1.1.1, Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 1: Requirements. Technical Specification (March 2010)
15. ETSI TS 102 636-2 V1.1.1, Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 2: Scenarios. Technical Specification (March 2010)
16. ETSI TS 102 637-2 V1.2.1, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service, Technical Specification (March 2011)
17. Filjar, R., Vidovic, K., Britvic, P., Rimac, M.: eCall: Automatic notification of a road traffic accident. In: Proceedings of the 34th International Convention MIPRO, pp. 600–605 (2011)
18. Geonet Project (2012), http://www.geonet-project.eu/
19. Hess, S., Segarra, G., Evensen, K., Festag, A., Weber, T., Cadzow, S., Arndt, M., Wiles, A.: Towards Standards For Sustainable IT. In: Europe. ITS World Congress (2009)
20. Intelligent Transport Systems, ETSI, http://www.etsi.org/WebSite/Technologies/IntelligentTransportSystems.aspx
21. ITU X.691, Information technology - ASN.1 encoding rules: Specification of Packed Encoding Rules (PER) (2011)
22. Jakubiak, J., Koucheryavy, Y.: State of the Art and Research Challenges for VANETs. In: IEEE Consumer Communications and Networking Conference, pp. 912–916 (2008)
23. Lee, K.C.: Geo-opportunistic routing for vehicular network. IEEE Communications Magazine 8(5), 164–170 (2010)
24. Mangel, T., Schweizer, F., Kosch, T., Hartenstein, H.: Vehicular safety communication at intersections: Buildings, Non-Line-Of-Sight and representative scenarios. In: International Conference on Wireless On-Demand Network Systems and Services (WONS), pp. 35–41 (2011)

25. Mannisto, D., Dawson, M.: An Overview of Controller Area Network (CAN) Technology; mBus (2003)
26. Miller, J.: Vehicle-to-vehicle-to-infrastructure (V2V2I) intelligent transportation system architecture. In: Intelligent Vehicles Symposium, pp. 715–720 (2008)
27. Preparation for driving implementation and evaluation of C2X communication technology (2011), `http://www.cvisproject.org/en/links/pre-drive_c2x.html`
28. Sepulcre, M., Mittag, J., Santi, P., Hartenstein, H., Gozalvez, J.: Congestion and Awareness Control in Cooperative Vehicular Systems. Proceedings of the IEEE 99(7), 1260–1279 (2011)
29. Unibaso, G., Del Ser, J., Gil-Lopez, S., Molinete, B.: A novel CAM-based traf-fic light preemption algorithm for efficient guidance of emergency vehicles. In: 13th International IEEE Conference on Intelligent Transportation Systems (ITSC), pp. 74–79 (2010)
30. Wang, Y., Teter, J., Sperling, D.: China's soaring vehicle population: Even greater than forecasted? Energy Policy 39(6), 3296–3306 (2011)

A Wireless Sensor Network for Early Warning of Elephant Intrusions

Lanka Wijesinghe, Prasanga Siriwardena, and Dileeka Dias

Dialog – University of Moratuwa Mobile Communications Research Laboratory,
Department of Electronic & Telecommunication Engineering
University of Moratuwa, Sri Lanka
{lanka,prasanga,dileeka}@ent.mrt.ac.lk

Abstract. A wireless sensor network (WSN) specifically designed for detecting elephant intrusions into villages that border wildlife reserves and alerting threatened communities of the location of the same is described. Novel strategies for hardware, firmware and communication have been applied, exploiting the rareness of events to be detected and the low data rates and light traffic load involved, in order to balance power consumption, cost, easy installation and testing in rural areas. Attempts have been made to build in automatic preventive maintenance measures and maintainable by personnel without technical know-how. The paper presents the design of the system and the experimental evaluation of a prototype implementation.

Keywords: Human-Elephant conflict, intrusion detection, energy efficiency.

1 Introduction

During the last 50 years, the human elephant conflict (HEC) has developed into one of the biggest environmental and socio-economic crises in Africa and Asia. Over the last four decades, the Asian elephant population has declined drastically, and the biggest threats to its survival are habitat loss and conflict with humans over crop raiding [1]. Today, it is one of the most endangered herbivores in the world.

Bangladesh, India, Kenya, Sumatra and Sri Lanka are among the countries hardest hit by the HEC. In Sumatra, villagers subject to repeated crop raiding and house destruction resort to poisoning elephants. In 1996 twelve elephants had been poisoned in Riau province. In May 2002, 17 elephants had been poisoned in North Sumatra [2]. In the State of Kerala as many as 704 elephants have died since 2003, which translates into an annual average of 120 elephants or one elephant killed every three days [4]. From 1992 - 2010, 1045 people were killed by elephants and 2,792 elephants were killed by farmers and from 2004 to 2007 a total of 3,103 homes were destroyed by elephants. The damages caused by elephants to crops in the area have been estimated to cost Rs. 1,100 million (US$10 million) annually [4].

Though the most well know solution to keep elephants out of human habitats is electric fencing, due to difficulties in maintenance of such fences, large segments are

F.K. Shaikh et al. (Eds.): WSN4DC 2013, CCIS 366, pp. 38–50, 2013.

not functional. As almost all intrusions occur at night, it is difficult to take preventive action. Once a breach has occurred, it is an extremely difficult task to locate it for repairs due to the length of the fences and the jungle territory they run through. Thus, fences go unrepaired and communities unprotected for long periods of time. Additionally, 70% of Sri Lanka's wild elephant populations live outside protected wildlife areas, sharing land with rural people and not separated by electric fences.

The wireless sensor network described here is developed to address the above issues. Ideally such a system should have the following capabilities:

- To detect elephant intrusions regardless of the presence or absence of an electric fence and without animal-borne sensors
- Energy efficient operation
- To be installed, maintained and repaired by trained, but non-technical personnel
- To be monitored remotely
- Devices should be low cost and robust in operation
- Be scalable to be installed along long perimeter boundaries of length 10 km or greater
- To issue alerts of intrusions and their locations to threatened communities
- To operate in areas with poor connectivity

2 Related Work

2.1 Fault and Intrusion Detection in Fences

Perimeter intrusion detection systems such as [5] have been researched and/or are available commercially. These are intended for securing locations such as airports and military bases and are not suited technically and economically for protecting wildlife fences extending over tens or hundreds of kilometers where severe energy constraints and harsh environmental conditions exist. Electric fences reported in [6] are accompanied by proprietary tools to detect faults. The information available indicates that only the direction of the fault is found with these tools, and manual methods are resorted to locate it. The technique reported in [7] locates each fault using manual voltage and current measurements along the fence. The alarm system in [8] consists of a number of detectors, each having a unique identifier. When the segment is broken, the detector transmits the identifier by means of an integrated antenna. Virtual fencing with animal-borne sensors is reported in [9], while an overview of virtual fencing techniques is presented in [10]. [11] Presents a comprehensive summary of research on event detection in wireless sensor networks, with applications in security.

Relevant prior work mostly deals with security and farm applications. Though energy consumption is an issue taken up in these works, the application scenarios are very different from the ultra low-power requirements of a sensor network in the wild. The cost of hardware used is also beyond the practical feasibility for jungle deployment.

2.2 Challenges of WSNs in Harsh Settings

The powerful combination of distributed sensing, computing and communication offered by WSNs, is presented in [12]. How WSNs lend themselves to countless applications and, at the same time, offer numerous challenges for practical deployment and the impact of hardware design of the nodes in terms of energy utilization, processor, communication hardware, and sensors are discussed in detail. [13] Discusses a number of system issues identified in taking laboratory WSNs into this type of environments such as deployment, unattended operation, and sensing range.

The work presented in this paper is a result of several design-pilot-refinement cycles by the authors of addressing the problem of elephant intrusions through electronic sensing mechanisms. Our previous effort has been presented in [14], which is a wired sensor network. The comparative advantages and disadvantages of the wired approach over wireless and many other lessons learnt through the experience in [14] have been applied in the improved design presented herein.

3 Design Overview

Figure 1. shows an overview of the system. The WSN which operates at 433 MHz consists of three types of devices functioning as outlined below:

- Sensors installed at known locations, which issue messages regarding system status or intrusions along with their identity.
- The RTU (Remote Transmitting Unit) which collects messages from the other devices via the WSN and relays them to desired destinations via text messages (SMS) over the mobile network. The RTU should be located where mobile network connectivity is present.
- Repeaters which provide radio connectivity between the sensors and the RTU as necessary. They carry messages from the sensors in a multi-hop fashion to the RTU.

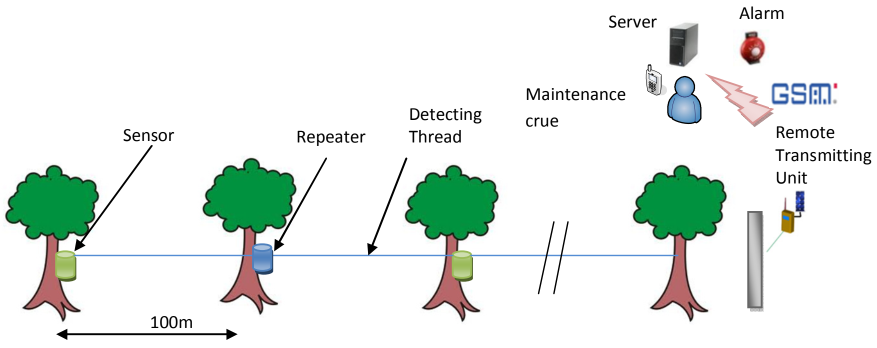


Fig. 1. Overview of the WSN

The sensors have a communication range of 100m, and may be spaced as necessary considering the cost and the sensing granularity. Repeaters have a communication range of 200m. They work to provide connectivity between the sensors and the RTU. A repeater will communicate with all sensors within a 100m radius and communicate with either the RTU or another repeater within a radius of 200m. The RTU is equipped with a 433 MHz transceiver for communicating with the WSN and a GSM interface for communicating via the mobile network. The end objective of the research is to cover a a span of 1 km with one RTU, four repeaters and ten or more sensors as required in order for energy and financial effectiveness.

4 Design Considerations

4.1 Assumptions

The following application-specific assumptions have been made in the design in order to simplify the hardware and communication protocol design. This in turn reduces cost and energy consumption.

- Intrusions are rare events.
- Triggering of more than three sensors concurrently is unlikely.
- As a result of the above assumptions, the WSN has an extremely light traffic load

4.2 Sensing Intrusions

Intrusion sensing is by shock detection. If the WSN is installed along an electric fence, the sensors may be mounted on the fence posts. In the event of an intrusion, the shock felt by the post is detected. If the system is to be installed without an electric fence, the sensors maybe fixed on trees along the periphery of the area to be protected as shown in Figure 1, and a non-conducting thread segment is drawn from one sensor to the next sensor position. The segment breaks during an intrusion, causing the sensor mounting mechanism to generate a shock on the connected sensor. The intrusion detection information is packetized and sent to either the RTU or a Repeater within range of the sensor. Several precautions are taken in order to minimize false triggering and sensor damage in the event of an intrusion such as a special mounting mechanism, thread drawn at a height such that small animals do not trigger it and a rugged PVC enclosure.

Though options such as wireless mechanisms, infra-sound, laser, cameras etc. were considered earlier on in the research, many are not feasible due to cost and power requirements for continuous sensing.

4.3 Ultra-Low Power Operation

The RTU and the repeaters are powered with small solar panels, and a common cell phone battery for back-up. Sensors are powered with two AAA size dry cells.

The sensors are in sleep mode normally. They wake up when a shock is detected and relay the message to the RTU or to the repeater within its reach. The RTU and the repeaters are also normally in sleep mode. When they are periodically woken up as described in Section 6 by an internal timer, they do the necessary tasks for data collection from the sensors and go back to sleep. Since the GSM modem is always active, the RTU draws a relatively high current in the sleep mode. The approximate currents drawn during sleep and active modes are summarized in Table 1.

Table 1. Currents drawn by WSN devices

Device	**Current in Sleep Mode (µA)**	**Current in Active Mode (mA)**			**Sleep/Wakeup cycle**
		TX	SMS send/rec	RX	
Sensor	15	89.5		23	Wakes up only when disturbed or once a day for health check. The maximum wake-up time is 12s.
Repeater	15	89.5		23	~2 s active, ≥ 8 s sleep
RTU	2000 - 2500	92	200	28.5	

4.4 Easy Installation, Monitoring and Maintenance

As the WSN is installed in environments which may be difficult to access, the health of the system should be monitored remotely. In the event of an intrusion, the system must be restored easily and quickly. Repair should be possible with low-cost locally available items. The responsibility of maintaining the system lies with the neighbourhood village community. In consideration of the above, installation, testing and maintenance as well as repair after an intrusion should be simple. The devices themselves carry out a health check once every 24 hours. The battery level is reported with every message generated by the sensors and repeaters during the daily routine health check as well as an intrusion. The results are reported to the maintenance crew via a text message. This report will indicate any malfunctioning devices and battery levels of all devices.

5 Hardware Design

The hardware design is summarized in Table 2. All devices are lower in cost and simpler in design compared to commercially available sensor nodes (motes). The motivation for the choices for key components is described in Table 3.

Table 2. Hardware design of WSN components

Device	Description
Sensor	The sensor consists of the MMA8452Q accelerometer chip for shock sensing, the low-cost RFM22B radio transceiver module and an ATmega88V low power 8bit microcontroller from Atmel. All components including the antenna are soldered on a 45mm x 27mm PCB. The board is powered with two AAA size batteries without regulators.
Repeater	The repeater hardware consists of an ATmega88V microcontroller, a RFM22B radio transceiver module and a small transistor based regulator used as a battery charger that charges the Lithium-ion BL-5C cell phone battery from a solar panel (9.0V, 70mA, 85mm x 69mm x 2.5mm LxWxD) mounted on the enclosure. All components excluding the solar panel and battery are soldered on a 40mmX64mm PCB. A XC6210B332MR 3.3V LDO regulator is used to power the board.
RTU	The RTU consists of an Atmel ATmega64L 8-bit microcontroller, a RFM22B radio transceiver module, a SIM900 GSM/GPRS module, a SIM holder, a XC6210B332MR 3.3V LDO regulator and a small transistor regulator for charging the BL-5C cell phone battery. A solar panel (9.0V 70mA 85mm x 69mm x 2.5mm LxWxD) is mounted on the enclosure. The PCB is of size46mmX64mm. A GSM antenna and a small wire antenna are mounted on the enclosure.

Table 3. Selection of Devices

Device	Major Motivation for selection
The RFM22B transceiver module	This is selected due to its low cost and high range compared to the other comparable radio modules. It also contains an ultra-low power RC timer that is used to wake up the microcontrollers in the RTU and repeaters (at10s intervals in the RTU and Repeaters and 24hour intervals in the sensors). It takes up much of the communications burden and enables the usage of low cost microcontrollers. It can also be configured to generate interrupts (such as valid packet received, transmission complete etc.) on its I/O pins which are used to implement the ultra-low power communication protocol.
The MMA8452Q accelerometer	This device consumes very low power in its sleep mode and has an inertial wake-up feature.
The SIM900 GSM module	This is a widely used low-cost, low-form factor GSM modules available. It also is very power efficient consuming 2.5mA in its sleep mode while being able to receive SMS.

6 The Communication Protocol

The objective of the communication protocol is for the RTU to collect either alarm packets generated due to an intrusion or routine health check packets from anywhere within the network. The packets so collected will be relayed over the mobile network to designated persons. Only the communication within the WSN is described here. The protocol has been designed with due consideration given to the following aspects:

- Low power consumption
- Collission avoidance
- Regular staus update (health check)
- On-site installation procedure

6.1 Protocol Description

The communication protocol is a receiver-initiated asynchronous duty-cycled protocol with a self-organizing time division multiple access scheme for Sensors. The RTU operates as a receiver. The Repeaters operate as both senders and receivers and the Sensors are senders. Messages originating at the Sensors are relayed in a multi-hop fashion to the RTU. The three modes of operation are the normal mode (no intrusion alarms or status update packets), the alarm/status update mode and the test mode. The key features of the communication protocol are described in Table 4.

Table 4. Key features of the communication protocol

Operation	Description
Normal Mode	Receivers within hearing range of each other execute a SEEK process asynchronously in a self-organizing, round-robin fashion. In this process, a burst of three SEEK packets (beacons) are broadcast at 10s intervals. Each of these are followed by a 2s listening (receive) interval. Three time slots are provided in each listening period (see collision avoidance). This constitutes the SEEK process as illustrated in Figure 2. In the normal mode, sensors remain in the sleep mode and there are no data packets travelling through the WSN.
Alarm/ Status Update Mode	When a Sender has data to send (an intrusion alarm or a routine status update in the case of a Sensor, or in the case of Repeaters, a packet received from a Sensor) it listens for a period of 12s for a SEEK packet. This policy ensures the reception of a SEEK from at least one receiver. On reception of the first SEEK packet, the Sender transmits the data packet in its time slot and waits for the ACK as illustrated in Figures 3and 4. If a Sender does not receive an acknowledgement, it retransmits its data in its time slot following the next SEEK in the same burst. This allows a Sender three transmission attempts. If a Repeater collects a data packet during its SEEK process it keeps on listening without sleeping until a seek from the next Repeater is received. Then it transmits the collected data to this repeater.

Table 4. (*Continued*)

Collision Avoidance	The RTU and Repeaters use a simple RC-timer which is prone to drift. At the time of power-up, the SEEK process is initiated. If a Repeater receives a SEEK packet of another Repeater or the RTU in its listening period, it automatically adjusts its SEEK time to move away from the other's SEEK. This reduces the possibility of collisions between SEEK packets. Following each SEEK, a maximum of three Senders can transmit data in three time slots without collision. The time slot assignment is computed as the modulo 3 division of the Sender's hardware address.

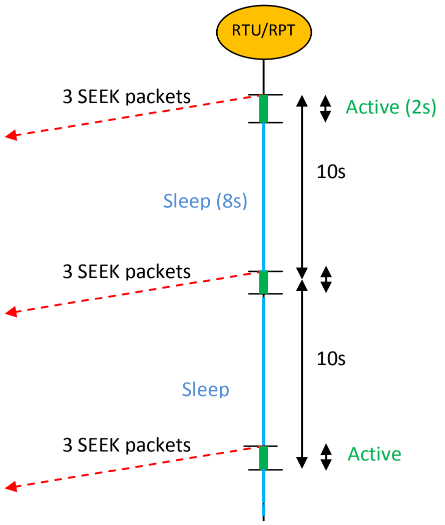


Fig. 2. The SEEK Process by Receivers

6.2 Selection of Parameters

SEEK Interval Estimation

The energy consumption is highest in the RTU. The SEEK interval is set to 10s for the RTU to operate without solar power (for example during a rainy period) for three days in the normal mode. In this mode, the energy expended to handle data packets is negligible compared to the GSM modem and the 24-hour SEEK process shown in Figure 2. The current in different modes drawn by the devices are presented in Table 1.

The SEEK interval can be made significantly larger in order to improve energy efficiency at the cost of packet latency, particularly in a long distance, multi-hop deployment.

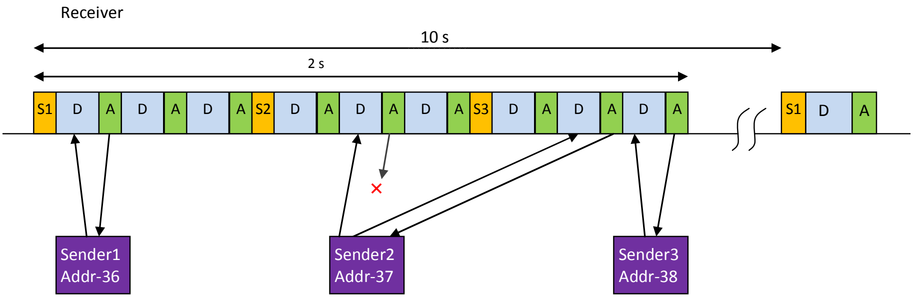


Fig. 3. Medium Access and Collision Avoidance (Sn:SEEK, D:Data, A:ACK)

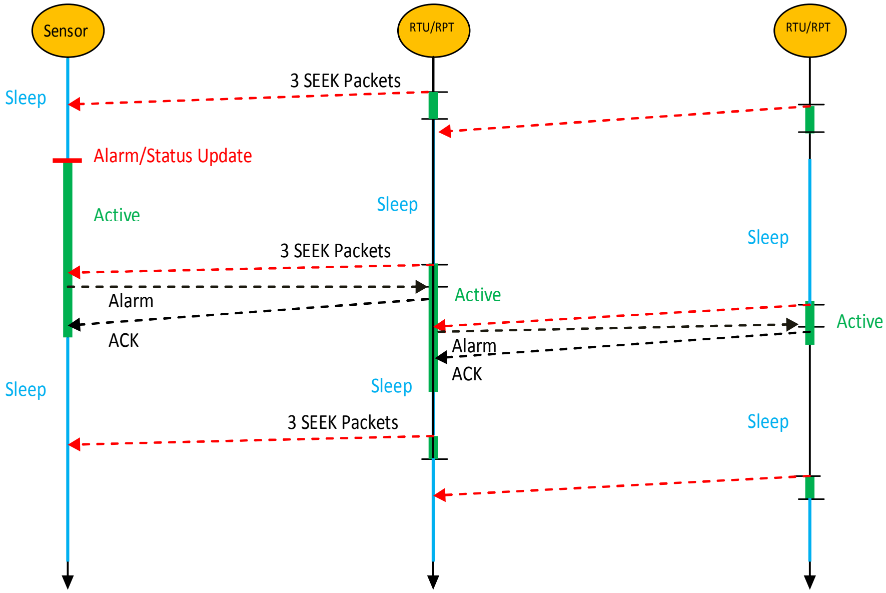


Fig. 4. The Alarm/Status Update Mode

Active Duration Estimation

After each SEEK packet, the receiver listens for data from senders. The listen period is divided into three slots to accommodate three senders. Each slot has length 124ms (74 bytes at 4.8kbps) for a DATA packet and 75ms (45bytes at 4.8Kbps) for the ACK. Therefore each slot is 199ms long. The Listen period for all three slots is 597ms. For the entire seek process, the active duration includes three SEEK packets and their listening times amounting to a total of 2016 ms (approx 2s).

6.3 Comparison with Other Protocols

Comparable ultra low-power duty-cycled MAC protocols for WSNs include RI-MAC [15], X-MAC[16] and WiseMAC[17]. X-MAC and WiseMAC are asynchronous and do not use receiver initiation. They have high power efficiency for light traffic loads and are based on the sender waking up periodically. RI-MAC is a versatile protocol which uses receiver initiation and is able to handle a wide range of traffic loads. These protocols are intended for networks of homogenous sensors.

The protocol presented here is for a specific application whose assumptions have been outlined in Section 4.1. In addition, a prime requirement was for the protocols to be implemented on low cost components with small internal memory. In our application, Sensors have extremely low power consumption and duty cycle, and are low cost battery operated devices present in large numbers in the network. The Repeaters and the RTU form the communication infrastructure. They are fewer in number, solar powered and can handle larger duty cycles. As such, we have borrowed several applicable features from the above protocols such as receiver initiation, and strobed SEEK packets and compiled a simple protocol with sufficient capabilities for the application.

7 Experimental Evaluation

Figures 5 and 6 show the RTU , Repeater and the Sensor.

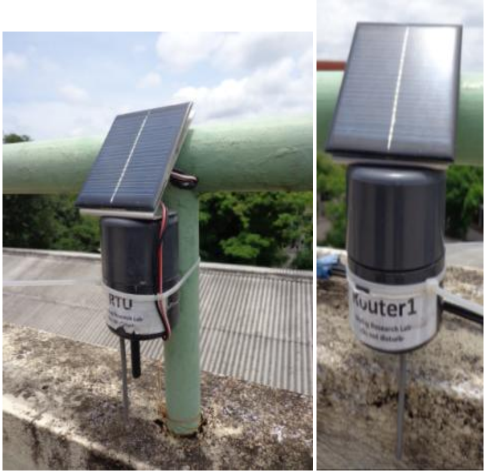


Fig. 5. The RTU (left) and a Repeater (right)

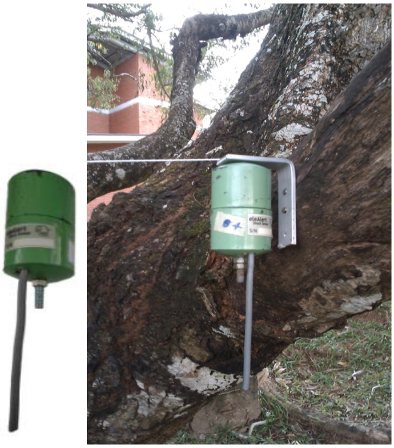


Fig. 6. The Sensor (left) and its installation (right)

7.1 Evaluation of Sensor Operation

The sensor operation (shock detection) was evaluated via a large number of manual shocks when mounted on a post as well as through the thread break mechanism. In all instances, the shock was detected. Thus, 100% accurate shock detection has been observed. Our calculations show that in the normal mode of operation, with one status packet sent per day by a sensor, the expected battery lifetime is 14 months.

7.2 Evaluation of Communication Protocol

A series of experimental deployments were carried out for evaluation. The deployment scenarios are summarized in Table 5. The environment and device locations are shown in Figure 7.

In each test, each Sensor in turn was made to repeatedly transmit an alert packet according to the communication protocol. The traversal of the packet through the network to the RTU was traced by a Listener. The Listener is a device similar to a Repeater, but has only the receive functionality. It enables the operation of the protocol to be viewed and recorded on a mobile device. Packet traversal to the RTU was extracted from the information gathered by the Listener as well as the reception of a corresponding text message. The results are presented in Tables 6 – 8.

Table 5. Experimental Deployment Scenarios

Scenario	Description
A	A system with an RTU and Sensors only. The path between the RTU and Sensors is shadowed by vegetation.
B	A system with an RTU and one Repeater. The Sensor was intentionally placed so that it is not able to hear the RTU directly.
C	A system with an RTU and three Repeaters. In the available location, the Sensors were able to hear all the Repeaters as well as the RTU.

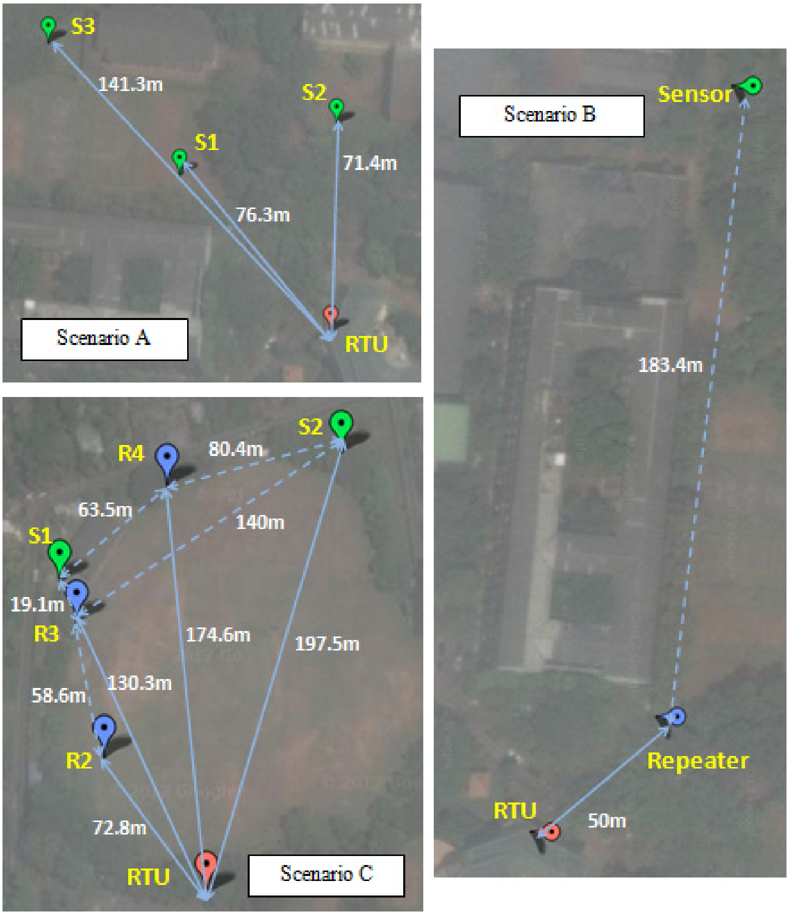


Fig. 7. Experimental Deployment Scenarios

In the case of direct communication between the sensors and the RTU in the absence of a repeater (scenario A), 100% successful packet reception was observed for ranges up to 100m. Thus, a repeater-less system can cover a circle of 200m diameter with one RTU. Beyond that the reliability drops, indicating the need for repeaters to extend the range. In the presence of a repeater as in Scenario B, 70% successful reception around an obstruction (a building) has been observed.

In Scenario C, where a number of Repeaters as well as the RTU were within hearable range of the Sensors, the packets travelling through several paths were observed as listed in Table 8. 100% successful traversal via two hops was observed from Sensor 1, whereas this failed in the case of Sensor 2. Single-hop traversal was seen to fail in some instances. Similar overall success rates were observed for both senders.

Table 6. Experimental Results for Scenario A

Sender	Packet Reception by RTU (%)
S1	100%
S2	100%
S3	90%

Table 7. Experimental Results for Scenario B

Sender	Packet Reception by RTU (%)
Sensor	70%

Table 8. Experimental Results for Scenario C

Path to RTU	Packet Reception by RTU (%)
From Sender S1	
R3-RTU	72
Directly to RTU	100
R2 -RTU	0
R3-R2-RTU	100
R4-RTU	70
Overall success	65
From Sender S2	
R3-RTU	67
Directly to RTU	83
R2-RTU	0
R3-R2-RTU	0
R4-RTU	71
Overall success	67

8 Conclusion

The paper presents the design and experimentation of a WSN for detection of elephant intrusions into human habitats. Our objective is to improve the effectiveness of electric fences and to provide a low-cost alternative to areas which do not have electric fences as a solution to the prevailing human-elephant conflict (HEC) in South Asia. To the best of our knowledge, this is a unique application of wireless sensor networks, and hence a novel contribution to the field.

The simple and inexpensive sensing mechanism has been demonstrated to be 100% reliable in terms of intrusion detection relevant to the present application. Deployment in a single RTU configuration without repeaters can cover a 200m span of perimeter reliably. Reliability needs to be improved for multi-hop communication over multiple Repeaters, which is essential for scaling up.

Acknowledgements. The authors are thankful to the Sri Lanka Wild Life Conservations Society (SLWCS) for their partnership in developing the concept, to M. Sumudu Hasala and Chandana Pushpakumara for assistance in testing and to the reviewers for their valuable feedback for improvement of this paper.

References

1. Sukumar, R.: The Asian Elephant: ecology and management. Cambridge University Press, Cambridge (1989)
2. Human Elephant Conflict, `http://elephantcare.org/humanele.htm#Humans%20killed`
3. One Elephant Dies Every Third Day, `http://archive.deccanherald.com/Content/Feb22009/scroll20090202116066.asp?section=frontpagenews`
4. Bandara, R., Tisdell, C.: The net benefit of saving the Asian elephant: A policy and contingent valuation study. Ecological Economic. 48, 93–107 (2004)
5. Electronic Fencing and Security Systems, `http://www.d-fence.com/`
6. Gallagher Animal Management Systems, `http://www.gallagher.com.au`
7. McGillan, G.: Design of an Electric Fence Fault Finder. M. Sc. Thesis, Massey University, New Zealand (2009)
8. Alarm system for electric fences, United States Patent 4523187 (1985)
9. Corke, P., Peterson, R., Rus, D.: Virtual Fences for Controlling Cows. In: Proc. of the IEEE International Conference on Robotics and Automation, ICRA 2004 (2004)
10. Umstatter, C.: The Evolution of Virtual Fences: A Review. Computers and Electronics in Agriculture 75(1), 10–22 (2011)
11. Wittenburg, G.: Cooperative Event Detection in Wireless Sensor Networks. The IEEE Communication Magazine 50(12), 124–131 (2012)
12. Puccinelli, D., Haenggi, M.: WSN: Applications & Challenges of Ubiquitous Sensing. The IEEE Circuits and Systems Magazine 5(3), 19–31 (2005)
13. Tannenbaum, A.S., Gamage, C., Crispo, B.: Taking Sensor Networks from the Lab to the Jungle. Computer 39(8), 98–100 (2006)
14. Wijesinghe, L., Siriwardena, P., Dahanayake, S., Kasthuriratne, D., Corea, R., Dias, D.: Electric Fence Intrusion Alert System (eleAlert). In: Proc. of the IEEE Global Humanitarian Technology Conference, Seattle, Washington, USA (2011)
15. Sun, Y., Gurewitz, O., Johnson, D.B.: RI-MAC: A Receiver-Initiated Asynchronous Duty Cycle MAC Protocol for Dynamic Traffic Loads in Wireless Sensor Networks. In: Proc. of the 6th ACM Conference on Embedded Network Sensor Systems, SenSys 2008, pp. 1–14 (2008)
16. Buettner, M., Yee, G.V., Anderson, E., Han, R.: X-MAC: A Short Preamble MAC Protocol for Duty-Cycled Wireless Sensor Networks. In: Proc. of the 4th International Conference on Embedded Networked Sensor Systems, pp. 307–320 (2006)
17. El-Hoiydi, A., Decotignie, J.-D.: WiseMAC: An Ultra Low Power MAC Protocol for Multi-hop Wireless Sensor Networks. In: Nikoletseas, S.E., Rolim, J.D.P. (eds.) ALGOSENSORS 2004. LNCS, vol. 3121, pp. 18–31. Springer, Heidelberg (2004)

Analysis of Wardriving Activity and WiFi Access Points

Elbaraa Eldaw[1], Akram M. Zeki[2,*], and Shayma Senan[3]

[1] Department of Information System,
Kulliyyah of Information & Communication Technology,
International Islamic University Malaysia, Malaysia
al.xase99@gmail.com
[2] Department of Information System,
Kulliyyah of Information & Communication Technology,
International Islamic University Malaysia, Malaysia
akramzeki@iium.edu.my
[3] Department of Electrical and Computer Engineering,
Kulliyyah of Engineering,
International Islamic University Malaysia, Malaysia
shay_sinan@yahoo.co.uk

Abstract. This paper proposes a system composed of hardware and software components that facilitates the activity of wardriving and assists in collecting statistical data by GPS of WiFi networks and their security status in particular area. The application has the potential of being used as a tool to study WiFi security trends or for misuse and WiFi exploitation.

Keywords: Wardriving, WiFi logging, WiFi Security, WiFi Statistics, Security Trends.

1 Introduction

Wireless networks are widely used nowadays. The use of WiFi technologies can be unsecure, thus new methods like wardriving were invented [1]. Wardriving is the method of searching for wireless LAN (WLAN) signals within a particular region. To do wardriving, a person needs a vehicle, a computer (which can be a laptop), a wireless Ethernet card, and some kind of antenna which can be mounted on top of or positioned inside the car [2]. The gathered information could be kept for personal use or shared with others. So, when a person needs to use free internet, he knows all the wireless points.

Traditional wardriving is ad-hoc and resultant datasets are composed of numerous passes by many drivers [3]. Wardriving is a controversial practice, but it has helped raise awareness of the importance of WLAN security. For example, many home networkers now configure Wireless Encryption Privacy (WEP) on their WLANs to block public access by wardrivers [4]. The scope of this study is to make a java based application that will facilitate the activity of wardriving by attaching a GPS module to a portable computer and writing code that will automatically store gps co-ordinates of wifi access points and their security status (unsecured/wep/wpa/wpa2). The hope was that this system would then enable one to generate a graphical map of collected access points.

F.K. Shaikh et al. (Eds.): WSN4DC 2013, CCIS 366, pp. 51–59, 2013.

Knowing open access points makes it an easy location to get free internet, knowing weakly secured access points (wep), makes it an easy target to attack and crack its password and then exploit the access point [5]. The system also had the potential of being made a mobile system as most smartphones come pre-equipped with gps modules. The objectives of this study are to increase the efficiency of wardriving, and to increase awareness of WLAN network security, also to create a technique of quickly capturing and logging statistical and location information of WLAN networks.

2 Related Works

There are many studies and researches have been done about war driving. In [6], accuracy and efficiency of war driving process had been studied using three different methods: on foot, on bicycle, and in car. Experiments show the position estimation's strong dependence on the particular means used for war driving.

WiFi signal characteristics have been used in [7] to identify when a device has moved from one location to another. They compare two observed channel responses and determine whether they belong to the same location. It does not attempt to extract features from responses and map them to locations, and hence it cannot be used for localization.

In [8], they characterize the error in location inference when localization is done using AP locations discovered from war driving. However, they do not propose any alternative solutions to war driving.

Drive-by localization [9] emphases on deriving more useful radio-based information from just the received signal strengths of war driving. A directional antenna on a steerable mount is used, with the signal strengths from a full-circle sweep recorded at each position. The angle-of-arrival of data frames from a given AP at each location is estimated by the direction of the strongest signal. Besides the time cost for this method, the actual costs of the hardware are quite significant.

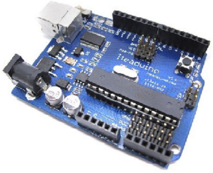
3 System Information

Table 1 shows the platform information to design the proposed system, while Table 2 shows hardware and equipment needed for the system.

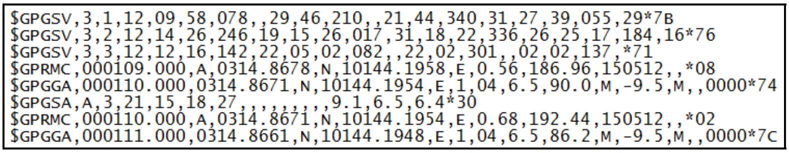
Table 1. Platform Information

Software Programming language:	Java
Hardware Programming language:	Arduinio
Operating System:	Windows 7 / Windows 8 tablet
IDEs Used:	Netbeans(Java) / Arduino Compiler (Arduino)

Table 2. Hardware and Equipment needed

GPS receiver:	20 Channel EM-406A SiRF III Receiver.	
Microcontroller used:	Arduino Duemilanove with an Atmega 328 microprocessor.	
Wi-Fi Device used:	Alfa AWUS036H	
Main Device used for capture:	Acer Iconia W501 tablet running windows 8 Preview	

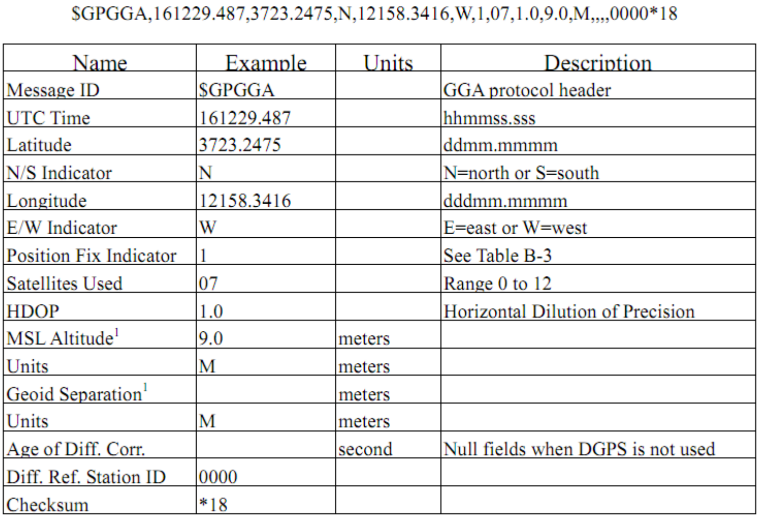
The microcontroller (Arduino) is necessary in order to interface with the GPS transmitter and receive the GPS co-ordinates. The Arduino board communicates with the computer by means of a USB (Universal Serial Bus) connection implementing Serial (UART) protocol communication. The system running on Java was designed to receive the string incoming from the Arduino board and decipher it to retrieve the GPS co-ordinates of the current location. An example of the string transmitted by the GPS device is shown in Figure 1.



```
$GPGSV,3,1,12,09,58,078,,29,46,210,,21,44,340,31,27,39,055,29*7B
$GPGSV,3,2,12,14,26,246,19,15,26,017,31,18,22,336,26,25,17,184,16*76
$GPGSV,3,3,12,12,16,142,22,05,02,082,,22,02,301,,02,02,137,*71
$GPRMC,000109.000,A,0314.8678,N,10144.1958,E,0.56,186.96,150512,,*08
$GPGGA,000110.000,0314.8671,N,10144.1954,E,1,04,6.5,90.0,M,-9.5,M,,0000*74
$GPGSA,A,3,21,15,18,27,,,,,,,,,9.1,6.5,6.4*30
$GPRMC,000110.000,A,0314.8671,N,10144.1954,E,0.68,192.44,150512,,*02
$GPGGA,000111.000,0314.8661,N,10144.1948,E,1,04,6.5,86.2,M,-9.5,M,,0000*7C
```

Fig. 1. Raw GPS sensor data

Only the GPGGA protocol is required to retrieve the information necessary. The GPGGA string is deciphered as shown in Figure 2.



$GPGGA,161229.487,3723.2475,N,12158.3416,W,1,07,1.0,9.0,M,,,,0000*18

Name	Example	Units	Description
Message ID	$GPGGA		GGA protocol header
UTC Time	161229.487		hhmmss.sss
Latitude	3723.2475		ddmm.mmmm
N/S Indicator	N		N=north or S=south
Longitude	12158.3416		dddmm.mmmm
E/W Indicator	W		E=east or W=west
Position Fix Indicator	1		See Table B-3
Satellites Used	07		Range 0 to 12
HDOP	1.0		Horizontal Dilution of Precision
MSL Altitude[1]	9.0	meters	
Units	M	meters	
Geoid Separation[1]		meters	
Units	M	meters	
Age of Diff. Corr.		second	Null fields when DGPS is not used
Diff. Ref. Station ID	0000		
Checksum	*18		

Fig. 2. GPGGA GPS protocol information

The programming for the GPS co-ordinate retrieval was done on the Arduino compiler. The Wi-Fi device used for this study was the Alfa AWUS036H. This device is used by many enthusiasts of Wi-Fi all over the world, it is a high performance device with heightened range and a variety of features. It is also well known for its advanced packet injection techniques and is used often to compromise the security of Wi-Fi access points. This Wi-Fi device was used as the device for detecting and analyzing the wireless signals detected.

4 Development Process

Figure 3 above shows the setup of the finalized system. The GPS device is placed in a box. Both the GPS device and the Wi-Fi adapter are connected to the tablet using a USB connection. The features of the system are:

- Captures Wifi SSIDs (Service Set Identifier) and BSSIDs (Basic Service Set Identifier) and their information.
- Captures GPS co-ordinates
- Plots GPS co-ordinate and detected access points on a map (if the access point has a signal strength of over 50%(modifiable value))
- Stores captured data to file.
- Stores captured data to MYSQL database.
- Detects whether or not the GPS device is connected.
- Data is logged at 5 second intervals (can be changed).

Information that is retrieved is displayed in a table, the information displayed in the table is as shown in Table 3.

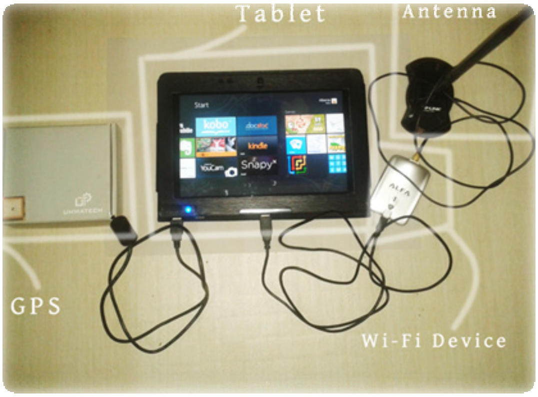


Fig. 3. System Setup

Table 3. Information collected by the system

Info	**Meaning**
SSID	Service Set Identifier (signal name)
BSSID	Basic Service Set Identifier (mac address)
SECURITY	Type of security implemented
ENCRYPTION	Type of data encryption implemented
SIGNAL STRENGTH	The strength of the wifi signal
CHANNEL	The channel of operation
DIRECT NET	Whether Direct internet connectivity is possible. (normally only for open access points that do not use a login gateway)
FILES	Are any files shared over this network (only applicable to open networks)

A test run of the system is shown below in Figure 4, conducted at the university campus.

A map was implemented with the help of the Google Maps API and embedded into the program where co-ordinates of access point detection is made and overlaid on top of the map for visualization of location.

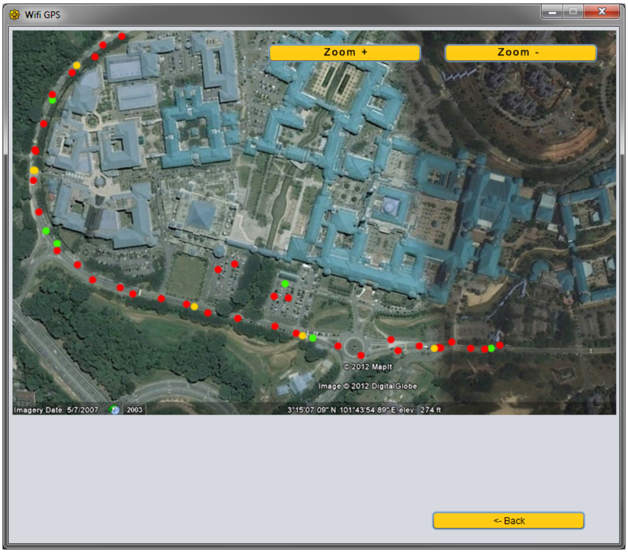
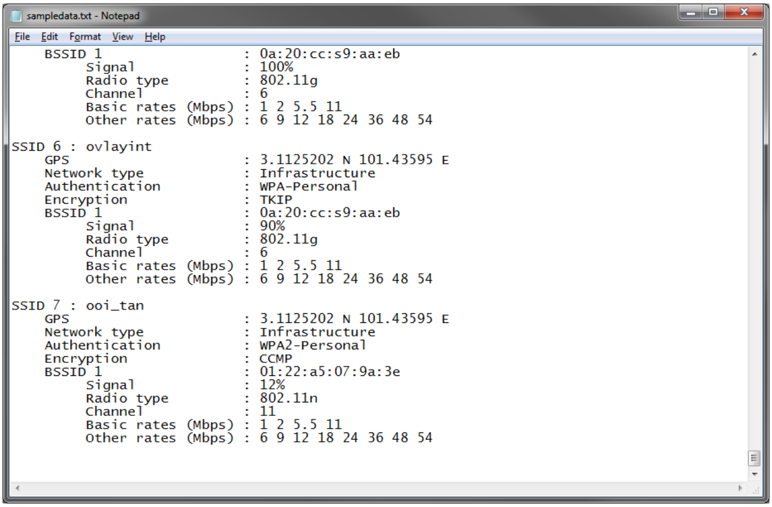

Wifi GPS
Zoom +
Zoom -
© 2012 MapIt
Image © 2012 DigitalGlobe
Imagery Date: 5/7/2007
2003
3°15'07.09" N 101°43'54.89" E elev 274 ft
<- Back

Fig. 4. Test run around the university campus

5 Results and Discussions

Figure 5 shown below presents a file of data sample captured by the system that will be used for analysis.



```
    BSSID 1                 : 0a:20:cc:s9:aa:eb
         Signal             : 100%
         Radio type         : 802.11g
         Channel            : 6
         Basic rates (Mbps) : 1 2 5.5 11
         Other rates (Mbps) : 6 9 12 18 24 36 48 54

SSID 6 : ovlayint
    GPS                     : 3.1125202 N 101.43595 E
    Network type            : Infrastructure
    Authentication          : WPA-Personal
    Encryption              : TKIP
    BSSID 1                 : 0a:20:cc:s9:aa:eb
         Signal             : 90%
         Radio type         : 802.11g
         Channel            : 6
         Basic rates (Mbps) : 1 2 5.5 11
         Other rates (Mbps) : 6 9 12 18 24 36 48 54

SSID 7 : ooi_tan
    GPS                     : 3.1125202 N 101.43595 E
    Network type            : Infrastructure
    Authentication          : WPA2-Personal
    Encryption              : CCMP
    BSSID 1                 : 01:22:a5:07:9a:3e
         Signal             : 12%
         Radio type         : 802.11n
         Channel            : 11
         Basic rates (Mbps) : 1 2 5.5 11
         Other rates (Mbps) : 6 9 12 18 24 36 48 54
```

Fig. 5. Data file containing collected data

The system was switched on while a car (Figure 6) was driven around the neighborhood to collect and process data.

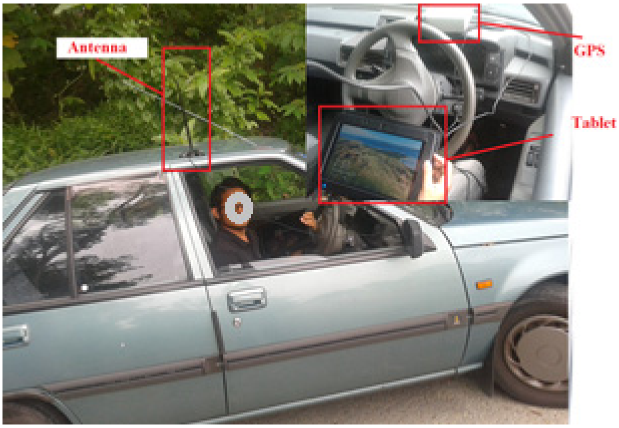


Fig. 6. System equipment on the car to be used for collecting data

The system's first field test was conducted in a residential neighborhood. Figure 7 shows the map generated after the test.

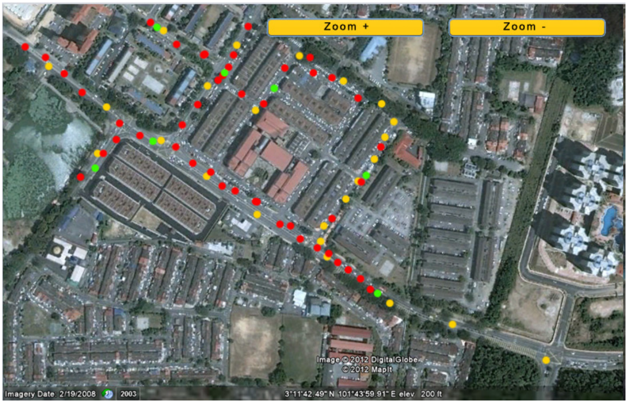

Zoom +
Zoom -
Image © 2012 DigitalGlobe
© 2012 MapIt
Imagery Date 2/19/2008
2003
3°11'42.49" N 101°43'59.91" E elev 200 ft

Fig. 7. Field test conducted at a residential neighborhood

The map in Figure 7 shows 3 colors:

- Red : Highly secured networks (WPA2 Enterprise, WPA2 Personal, WPA Enterprise).
- Yellow : Weakly secured locations (WPA Personal, WEP).
- Green : Unsecured (Open for access).

When testing, it was initially found out that if the system tried to log all access points it would cause a situation where many points overlap each other in one GPS location and that meant the colors of points below are unseen. The issue was rectified by implementing a tolerance, if the access point signal strength is below 50%, it is not plotted. This is also useful as any access point that has low signal strength is probably not good from that location anyway.

The general results of access points detected in the first field test were as follows:

- 178 Access points detected.
- 48 weakly secured (WEP).
- 17 unsecured.
- 9 have free internet access.
- 5 have shared files on an unsecured network.

WEP is a form of WiFi security that was found to have many weaknesses. WEP uses an encryption approach and the algorithms used proved too simple and can be cracked in a short time by an attacker [10].

6 Conclusion

With easily available GPS devices and stronger wifi analysis tools, the threat of WiFi predators will remain until more measures are taken to bring awareness to the issue and educate residents about the potential dangers that they could face should their networks be exploited. The potential for the system designed in this paper is wide and varied. A simple possible situation is where a community is born with the sole purpose of updating co-ordinates of Wi-Fi access points and their statuses to an online database that is shared by like-minded individuals. With the advent of more powerful hand held devices with better GPS tools and WiFi radios, one may soon not even need a setup that is as complex as the one set up here to perform such an analysis. This method of analysis could also be used for statistical collection of information for more awareness oriented measures.

References

1. Kim, M., Fielding, J.J., Kotz, D.: Risks of Using AP Locations Discovered Through War Driving, Department of Computer Science (DartmouthCollege) (2006)
2. Lawrence, E., Lawrence, J.: Threats to the mobile enterprise: jurisprudence analysis of wardriving and warchalking. In: Proceedings of the International Conference on Information Technology: Coding and Computing, ITCC 2004, April 5-7, vol. 2, pp. 268–273 (2004), doi:10.1109/ITCC.2004.1286645
3. Jones, K., Liu, L.: What Where Wi: An Analysis of Millions of Wi-Fi Access Points. In: IEEE International Conference on Portable Information Devices, PORTABLE 2007, May 25-29, pp. 1–4 (2007), doi:10.1109/PORTABLE.2007.45
4. Hurley, C.: WarDriving Drive, Detect, Defend: A Guide to Wireless Security. Syngress Publishing, Massachusetts (2004)
5. McClure, S.: Hacking Exposed 6: Network Security Secrets & Solutions. McGraw Hill, New York (2009)
6. Yoshida, H., Ito, S., Kawaguchi, N.: Evaluation of pre-acquisition methods for position estimation system using wireless LAN. In: Proceedings of the Third International Conference on Mobile Computing and Ubiquitous Networking, ICMU 2006, London, UK, pp. 148–155 (October 2006)

7. Zhang, J., et al.: Advancing wireless link signatures for location distinction. In: MobiCom. ACM (2008)
8. Kim, M., Fielding, J.J., Kotz, D.: Risks of using AP locations discovered through war driving. In: Fishkin, K.P., Schiele, B., Nixon, P., Quigley, A. (eds.) PERVASIVE 2006. LNCS, vol. 3968, pp. 67–82. Springer, Heidelberg (2006)
9. Subramanian, A.P., et al.: Drive-By Localization of Roadside WiFi Networks. In: IEEE The 27th Conference on Computer Communications, INFOCOM 2008, pp. 718–725 (2008), doi:10.1109/INFOCOM.2008.122
10. Peng, H.: WIFI network information security analysis research. In: 2012 2nd International Conference on Consumer Electronics, Communications and Networks, CECNet, April 21-23, pp. 2243–2245 (2012), doi:10.1109/CECNet.2012.6201786

Medical Body Area Network, Architectural Design and Challenges: A Survey

Madiha Fatima, Adnan K. Kiani, and Adeel Baig

School of Electrical Engineering and Computer Science (SEECS),
National University of Science and Technology (NUST), Islamabad, Pakistan
{11msitmfatima,adnan.khalid,adeel.baig}@seecs.edu.pk
http://seecs.nust.edu.pk

Abstract. Medical body area network is a human-centric application of wireless sensor network which has recently gained much significance. The application includes both wearable and implantable sensors for continuous monitoring of patients in hospitals, old houses or at any remote location. These sensor nodes in medical body area network possess all the characteristics of nodes in wireless sensor network. In this paper a survey of medical wireless body area network, its architectural design issues and challenges have been discussed.

Keywords: Wireless sensor network, medical body area network: architectural design, reliability, energy efficiency and routing.

1 Introduction

Body area network is a subcategory of wireless sensor network for monitoring physiological conditions around human and animal body. It has many human-targeted applications such as sports, entertainment and healthcare etc. Medical body area network keeps track of patients' vital signs in hospitals, in homes and even when patients are mobile through continuous real-time monitoring to provide healthcare services to them. For better understanding of technology, first we will introduce wireless sensor network then body area network and its healthcare applications.

Wireless Sensor network is composed of thickly inhabited tiny sensors which interact with the environment by sensing or monitoring it and pass their data to a base station for further processing and controlling actions. It has a wide variety of applications [1] including but not limited to industry, agriculture, habitat, forest and environmental monitoring, home and office automation, healthcare and medicine, urban sensor network and energy management etc. It can also be used in the application areas of security, defense, military and disaster monitoring. Its healthcare applications [2] include home-based care, hospital or clinical monitoring, management of disaster relief and medical facility, sports health etc.

Sensor nodes in wireless sensor network are small in size and memory, low cost, low power, and equipped with low processing and computing power. These nodes are of two types i.e. source node which monitors the environment and sink

F.K. Shaikh et al. (Eds.): WSN4DC 2013, CCIS 366, pp. 60–72, 2013.

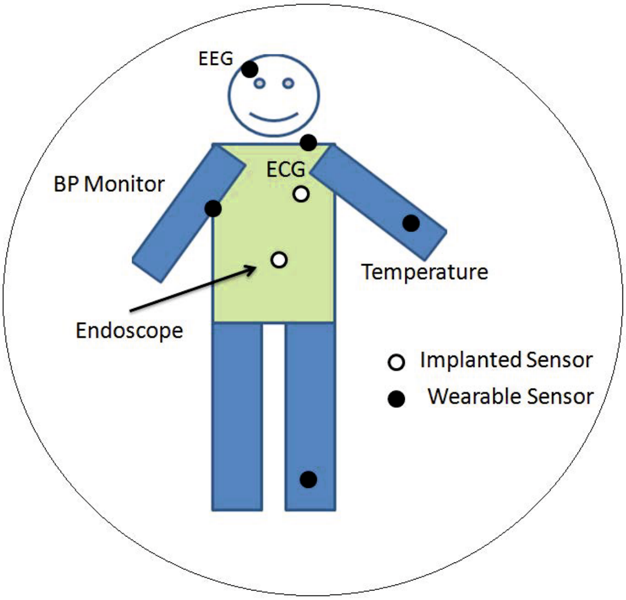


Fig. 1. Placement of sensor nodes on human body

which collects the information from the source and sends to base station. These nodes can be mobile depending on the nature of the application. In temperature monitoring application nodes are usually static and some applications like flood forecasting, transportation monitoring etc contain mobile nodes. Mobility can be categorized as sensor mobility, sink mobility and event mobility. Sensor nodes can be mobile to monitor a region or sense a phenomenon. For sink mobility it might be possible that a sink node is not a part of wireless sensor network e.g. PDA or laptop which remain mobile. The event can also be mobile. E.g. water in a river. There is a data centric communication in wireless sensor network which can be either in single-hop or multi-hop fashion [3]. Single hop communication supported in Bluetooth based wireless sensor network uses star like topology. In multi-hop communication relay nodes are involved which cooperatively pass on data to sink node. It is supported in ZigBee based wireless sensor network. Communication models used in wireless sensor network are periodic, event driven and query driven. In periodic data communication, sensor node periodically senses and sends data to the sink node e.g. monitoring weather, temperature etc. In a query based communication sensor nodes only transmit data when they receive any request from the sink node. In an event driven communication, sensor nodes only become active when a certain event occurs e.g. rise in temperature to threshold level etc.

Medical body area network slightly differs from other applications of wireless sensor network. Placement of sensor nodes on human body is shown in Fig. 1. Both internal and external sensors [4] are used for monitoring patient's vital signs. Internal sensors are ingestible or implanted devices e.g. core body temperature sensor. External sensors are wearable or detachable electrical signaling devices e.g. pulse OXIMETER, ECG, EEG sensors etc. Sensor nodes in medical body area network possess all characteristics of wireless sensor network and are of two types i.e. source and sink which can be static or mobile. For example in ICU rooms patients are static and in emergency rooms patients can be mobile where they are waiting for a checkup. Communication model used in medical body area network mainly depends on the patient's condition. Similarly sensor nodes in the network can communicate with each other either in single hop or multi-hop manner. Topology is usually known and communication is hybrid because some patients need continuous monitoring and some non critical patients need only periodic or query based reporting. In medical body area network information is identity centric [5] because data comes from different sensors which belong to different patients.

There are already very well known and comprehensive surveys on body area network (e.g., [6],[7],[8],[9],[10]) which focus on challenges and open research areas such as topology issues, MAC and physical layer issues and routing challenges etc. These surveys are generic and give a broader overview of body area network. We surveyed body area network to highlight research challenges specific to patient monitoring applications. Different telemetry systems are used in hospitals for patient monitoring such as In Vivo medical telemetry systems, Philips IntelliVue telemetry system, GE healthcare telemetry system etc. In these telemetry systems monitoring devices are attached to transceivers via wires on the cost of patient comfort. These transceivers transmit the patient data to receiving devices which further forward this data to base station where it will be accessible to doctors or caretakers. These telemetry systems are very costly and also involve wiring to some extent. Developing countries have limited resources and are very deficient in education and healthcare facilities. People in developing countries are very prone to diseases due to poor living conditions and food quality. Patient monitoring using wireless sensors would become a very cost-effective system for developing countries. These systems also provide ease of mobility to patients along with continuous and real time monitoring of their vital signs. Medical body area network is facing many research challenges related to architecture, energy efficiency reliability, MAC, network and physical layer issues. In our survey we focused on research challenges of reliability, energy efficiency and routing in medical body area network. We also highlight some applications of body area network for patient monitoring and architectural designs and its related issues.

We have organized the rest of our paper as follows: Section 2 covers some application examples of medical body area network for patient monitoring. Section 3 presents the functional architecture and section 4 presents challenges in medical body area network which includes the reliability, energy efficiency and routing. Section 5 includes the recommendations for overcoming the challenges in medical body area network. In section 6 we emphasize research and technology related challenges of medical body area network in developing countries. We present the conclusions in Section 7 followed by reference listing.

2 Medical Body Area Network

Many systems have been proposed for remote or hospital monitoring of patients. One example is SMART (Scalable Medical Alert Response Technology) a hospital monitoring system proposed by Dorothy et al. [11] which integrates wireless patient monitoring, geographical-positioning, signal processing, targeted alerting, and also wireless interfaces for doctors and caretakers. It is implemented in waiting or emergency rooms for monitoring of the patients who are sitting there and waiting for a checkup and medical aid. Similarly Jeonggil et al. [12] presented a network model MEDiSN for emergency detection using wireless sensor network. MEDiSN is developed for hospital and disaster monitoring. In this model relay points are used to carry and pass on the data in multi-hop fashion. Octav et al. [13] discuss the shortcomings of MEDiSN and conclude that the sensing reliability of body area network has been ignored in MEDiSN which is more critical as compared to network reliability in body area network. This paper represents the deployment of wireless clinical monitoring system for monitoring of pulse rate and oxygen saturation rate of patients. Sharma et al. [14] presented a prototype for remote monitoring of medical vital signs of a patient i.e. ECG, breathing rate and body temperature. This paper presented the implementation of body area network in beacon mode in which network coordinator wakes up the sensor nodes to sense and transmit the data to base station.

The first step towards medical body area network is to design an efficient, cost effective and robust architectural design. There are many distinct features of the medical body area network architecture which makes it unique from other wireless sensor network applications. Limited numbers of sensors are strategically located on human body to sense different types of data. In the following sections we will discuss some architecture of body area network and their design issues.

3 Functional Architecture

A basic functional architecture of the medical body area is shown in Fig. 2 in which patient's data is transmitting to the base station via relay node from where authorized doctors can access it for taking the necessary actions. Relay node also sends the data to monitoring or nursing room and triggers alarms here if any patient's condition goes critical. A data driven architecture of the medical body area network is proposed by Yuan-Jen et al. [15] which divides the network into two parts. In the first part communication is between sensor nodes and database and in the second part between the database and user interface. The sensor node senses data in periodic or event driven environment but transmission will be demand based. Users have no direct control and they update or acquire information from the sensor nodes via web applications. In paper [16] authors presented the comparison between 1-hop star and 2-hop extended star architectures and concluded that not any architecture fits the environment. They gave some guidelines to effectively design body area network. Similarly Yu Ge et al. [17] investigated the impact of single hop star and multi-hop architecture designs and concluded

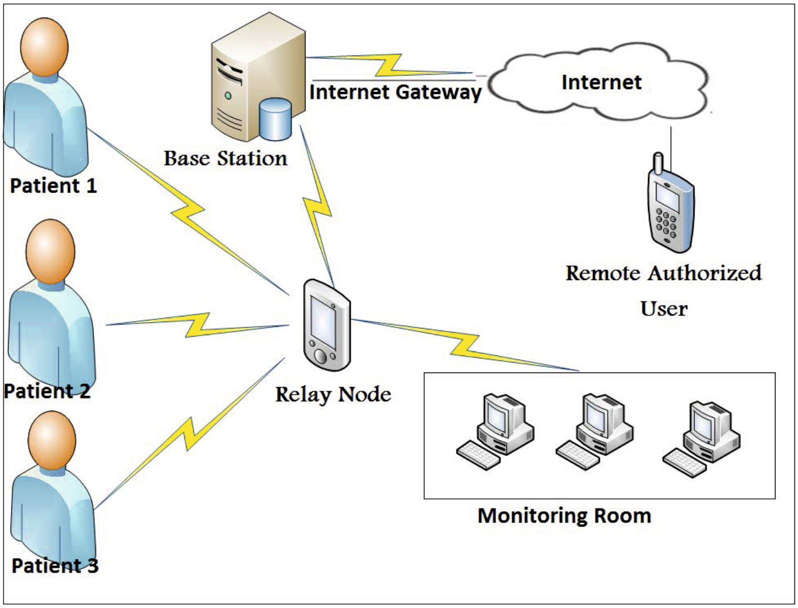


Fig. 2. Functional Architecture of Medical Body Area Network

that for reliable transmission of data multi-hop network architecture is efficient as compared to star architecture. Maha et al. [18] proposed a service oriented design for middle ware in body area network for continuous monitoring in care rooms or in old houses which also allow small scale mobility to patients. Sun et al. [19] presented architecture for medical body area network where different types of data are collected from patients. Network coordinator merges the data and sends it to the data centre or monitoring system.

There are many challenging requirements to be considered by designers while designing architecture of the medical body area network. For example appropriate placement of sensor nodes and relay nodes to reduce the interference so they can efficiently communicate with each other. To decide the number of sink nodes and their selection is a quite difficult task. The gateway provides connectivity to body area network towards other networks and internet. It is another challenge that which gateway approach should be used for body area network i.e. single gateway or multiple gateway approach. Architecture should be designed in a way they it should be robust and have the capability to resume from failures within very short time. Network failure of one unit could not affect the functionality of the other network. Besides architectural issues medical body area is facing critical research challenges such as energy efficiency, reliability and routing which should be addressed carefully. In the following section we will discuss these issues briefly.

4 Challenges

Due to limited power supply of nodes and critical nature of patient's data both energy efficiency and reliability have become very crucial issues. Routing is important in a way that it should consume minimum network resources. Following subsections present some related work of energy efficiency, reliability and routing in medical body area.

4.1 Energy Efficiency

Reason for sensor nodes being limited in power resources is their inexpensive nature and small size. Many protocols are introduced for power saving in medical body area network. Omeni et al. [20] proposed a MAC protocol for medical body area network which achieves energy efficiency simply avoiding collisions in the network by using an algorithm called clear channel assessment which is based on listen-before-transmit. HyungTae et al. [21] proposed an energy efficient MAC scheme in which a coordinator node controls the medium access by periodically sending beacon packets in order to synchronize the time slots among sensor nodes. Moshaddique et al. [22] proposed energy efficient MAC protocol which uses additional radio circuit to wake up the nodes. Using TDMA with wake up signal reduces the chance of collision and also increases the sleep time of nodes with acceptable packet delay. Sensor devices used in medical body area network can be broadly classified as wearable and implantable devices. To accommodate all types of devices in a single network is also a big challenge. In this context Timmons and Scanlon presented a medical MAC protocol named MedMAC [23] for energy efficiency and adaptability of channel access in medical body area. It uses TDMA for periodic data and also contains support for emergency data. An adaptive guard band algorithm is used to maintain the synchronization between nodes during their sleep.

Energy efficiency is a very important requirement of medical body area but it is still facing many research challenges. Algorithms for improving energy efficiency can cause unacceptable reliability issues, delays, latency for example duty cycles to avoid overhearing or idle listening. Turning radios on/off in sleep scheduling mechanisms consumes maximum energy. Both energy efficiency and reliability are controversial issues and we will have to draw a balance line of tradeoff between them. Techniques for ensuring reliability such as redundant data, retransmissions or acknowledgments utilize more network resources. In the following section we will discuss reliability then we will have a clear picture of these issues.

4.2 Reliability

Reliability in the detection and reporting of event is very critical because the patient's data is very sensitive in body area network. Other than network reliability sensor and software reliability is also a very important requirement. Software which maintains network devices, patients data and alarm systems should be robust to failure and available all the time. Octav et al. [24] proposed a mechanism named DRAP to cope with the patients mobility in clinical monitoring using wireless sensor network for achieving first hop reliability on the cost of energy efficiency. A cooperative network coding scheme is proposed in [25] in which network coding and cooperative communication are combined for many to many network configurations which reduces the probability of packet loss and increases network throughput. This scheme also avoids the single point of failure. Increasing number of nodes decreases the performance of the network because single transceiver devices cannot handle the growing traffic in the network. Ivanov et al. [26] proposed an approach to solve this problem by introducing multiple channels at MAC layer along with multi-hop cooperative communication between medical and environmental sensors. Sampangi et al. [27] proposed a scheme to reduce the network delay and packet loss by introducing multiple intermediate sinks. This scheme also reduced the contention between the sensor nodes for single sink node. Octav et al [13] highlighted the deficiency of MEDiSN [12] and proposed oversampling to ensure sensing reliability. They also used an alarm system to inform if any sensing device disconnected from the system. Similarly MedMAC [23] which accommodates multiple types of sensors in the network for energy efficiency and adaptability of channel access is also ensuring the node reliability. Dongheui et al. [28] proposed a two level communication scheme to provide reliable data transmission in medical body area network. In proposed scheme different RF bands are used for communication of sensor nodes to gateway and from gateway to base station. They also developed software and hardware platforms to support this two level scheme which is composed of sensor nodes, gateway and data server. The software platform composed of network protocols, kernel and application layer. Stepan et al. [29] proposed virtual grouping medical body area network for quality of data and it's analysis. They also introduced a new parameter called quality of health monitoring to take feedback from the doctors on data quality.

The reliability mechanisms cause more energy consumption which reduces the network's lifetime. For ensuring sensing reliability using oversampling cause more energy consumption due to multiple transmissions. It also causes redundancy and overburdens the sink nodes to receive and handle the increasing amount of data. In case of network or hardware failure how will it resume, how much time it will take to resume and what type of the backup should be available are also challenges for reliability. Reliability and energy efficiency are important factors but routing is also attention-demanding in medical body area network. Medical body area network requires a routing protocol which provides reliable and energy efficient end to end data delivery.

4.3 Routing

A routing protocol for healthcare application of wireless sensor network must have support for both periodic and event driven data. Support for periodic data is necessary to continuously monitor the data and event driven data for reporting the vital signs of patient to the doctor is necessary for in time treatment of patients. Routing protocols in healthcare monitoring can be categorized [30] as (1) periodic sampling, (2) event-driven monitoring and (3) hybrid monitoring. LEACH is a proactive protocol in which nodes periodically send their data to base station. TEEN is another cluster based algorithm which is reactive protocol for event driven monitoring. APTEEN is a hybrid protocol developed to merge the properties of both LEACH and TEEN protocols. Many sensors in the body area network monitor same observation region and have the same type of information. A routing scheme has been proposed [31] which selectively collects information from the nodes to reduce burden on the sink node by reducing transmissions in the network. Ababneh et al. [32] proposed energy-balanced rate allocation and routing protocol in medical body area network for load balancing and efficient rate allocation to nodes. EBRAR protocol builds a routing path on the basis of residual energy of nodes. Energy-balanced rate allocation and routing protocol force the packet to route through a path with nodes of higher energy towards the sink node. In this way it protects the nodes having lower residual energy. The proposed algorithm not only conserves the bandwidth of the system but also allows the nodes to transmit the data more intelligently and equally divides the burden of data transmission. C-AODV [33] is a routing algorithm for monitoring system which is based on cooperative communication among the nodes to obtain good performance tradeoff between the energy efficiency and reliability in the network. Hello message is sent to neighboring nodes for the purpose of acquiring informing about the node's queue length. On the basis of congestion in queue length the nodes take the decision of selecting a next hop for required destination. Quwaider et al. [34] proposed routing algorithm for location based store-and-forwarding of packet with frequent postural partitioning which provides the better routing delay performance. In order to reduce the electromagnetic interference from wireless sesnsor network in healthcare applications Quang et al. [35] proposed an adaptive and distributed routing protocol called EMI-aware routing protocol (EMIR). The algorithm assigns a positional value to each node. On the basis of this calculated value the traffic is diverted from the nodes with high electromagnetic interference or which are located far away from the gateway. Security is also an important feature in the medical body area network. Security concerns and threats can cause patients to suffer dangerous conditions or even death. Xiaohui et al. [36] proposed a routing protocol called distributed prediction based secure and reliable routing framework which provides reliability and prevention against the data injection attacks e.g. denial-of-service attack etc.

Routing is first step which will be performed in body area network. Sensing and transmission of data come next to it. All the steps involving in routing process such as neighbor discovery, maintenance of routing tables and path discovery and path maintenance all are resource consuming process. Reactive routing protocols cause delay in communication while proactive protocols cause so much utilization of network resources. Selection of appropriate routing protocols which should be reliable and energy efficient is still a question mark in research and needs to be addressed carefully.

5 Recommendations

Reliability is the most important requirement and critical issue in medical body area network. In star topology there is a single point of failure and it can cover only a small area. Nodes which are located at a long distance from the cluster head require a larger transmission range. Multi hop communication is a good option for ensuring communication reliability. For sensor reliability alarms should be introduced if devices disconnected from the network and there should be some mechanism to check the reliability of sensing data. For software reliability there should be back-up in case if the software fails. All the network devices which have a direct electricity supply should have backup energy resources so that network should be available all the time if an electrical failure occurs.

In the body area network energy efficiency and reliability are especially critical at first hop where there is communication between sensors and relay nodes. Sensors have limited power supply and can also be mobile while relay nodes are intelligent devices and are rich in resources i.e. power supply, processing and computing power etc. We can divide the network into two parts. At the first hop there is need of high reliability and energy efficiency and we can focus on this part. In the second part there will be communication between relay nodes and gateway to send the data to the base station over wired or wireless channel. Energy efficiency is not a big problem because the devices are having rich resources. Here we can focus on reliable data transmission and solving the interference problem.

The medical monitoring application involves transmission of vital signs of patients to the central base station. The main requirement in medical body area network is transmission of data so routing in the network should not be resource and bandwidth hungry. Building and maintenance of reliable routes should be efficient enough so that we can save energy in the routing and use it in communication of vital signs. At some points in the network we need proactive routing schemes and sometime we need reactive routing. The proactive routing scheme is more energy consuming and has larger overhead. We have to efficiently select the routing scheme in order to achieve energy efficiency but not on the cost of reliability in the network.

6 Challenges for Developing Countries

Medical body area network is very helpful and cost effective assisted living application. Developing countries can use this technology to improve the healthcare facilities for their people. Besides technology related issues medical body area network can face some extra challenges while introducing in developing countries. Implementation of this technology should be cost effective. Training of medical staff to use this system is an important task. There might be a possibility that users will be reluctant to use new technology. There are some issues specifically related to requirement of market research. User-friendliness, cost effectiveness, interoperability and compatibility of the medical body area network are key challenges for gaining market placement in developing countries. Many questions can arise for market placement that who will be expected buyer of this system? Who will be liable for damages and malfunctioning of system? What will be an acceptable cost for both customers and stakeholders? Who will be the owner of patients data in hospitals? Who will be able to access the data of the medical body area network? All these points should also be considered for implementing this technology in developing countries.

7 Conclusion

In this paper we have discussed the common properties of wireless sensor network and presented a survey of its health related applications. We have surveyed of medical body area network and discussed its implementation in hospital for clinical monitoring and disaster relief. We also discussed architectural design and challenges of body area network. While discussing the challenges in body area networks applications in healthcare we have touched upon reliability, energy efficiency and routing as these are the issues of great interest. There is a tradeoff between reliability and energy efficiency. There is a need to develop an efficient communication protocol which achieves both reliability and energy efficiency at an acceptable tradeoff level. We also discussed the benefits of introducing medical body area network in developing countries and challenges regarding this context.

References

1. Arampatzis, T., Lygeros, J., Manesis, S.: A Survey of Applications of Wireless Sensors and Wireless Sensor Networks. In: Proc. 13th Mediterranean Conference on Control and Automation, Limassol, pp. 719–724. IEEE Press, New York (2005)
2. Zhou, B., Hu, C., Wang, H.B., Guo, R., Meng, M.Q.-H.: A Wireless Sensor Network for Pervasive Medical Supervision. In: Proc. IEEE International Conference on Integration Technology, Shenzhen, pp. 740–744. IEEE Press, New York (2007)
3. Zheng, T., Wang, S., Kamel, A.E.: Bluetooth communication reliability of mobile vehicles. In: Proc. International Conference on Fluid Power and Mechatronics, Beijing, pp. 873–877. IEEE Press, New York (2011)
4. Lee, H., Park, K., Lee, B., Choi, J., Elmasri, R.: Issues in data fusion for healthcare monitoring. In: Proc. 1st International Conference on Pervasive Technologies Related to Assistive Environments, Athens, pp. 3:1–3:8. ACM, New York (2008)
5. Willig, A., Hauer, J.-H., Karowski, N., Baldus, H., Huebner, A.: The ANGEL WSN Architecture. In: Proc. International Conference on Electronics, Circuits and Systems, Marrakech, pp. 633–636. IEEE Press, New York (2007)
6. Min, C., Gonzalez, S., Vasilakos, A., Huasong, C., Leung, V.C.: Body area networks: A survey. In: Proc. Mobile Networks and Applications, pp. 171–193. Kluwer Academic Publishers, Hingham (2011)

7. Latré, B., Braem, B., Moerman, I., Blondia, B., Demeester, P.: A survey on wireless body area networks. In: Proc. Ireless Networks, pp. 1–18. Kluwer Academic Publishers, Hingham (2011)
8. Lee, H., Park, K., Lee, B., Choi, J., Elmasri, R.: Enabling technologies for wireless body area networks: A survey and outlook. IEEE Communications Magazine 47(12), 84–93 (2009)
9. Ullah, S., Higgins, H., Braem, B., Latre, B., Blondia, C., Moerman, I., Saleem, S., Rahman, Z., Kwak, K.S.: A comprehensive survey of wireless body area networks. Journal of Medical Systems 36(3), 1065–1094 (2012)
10. Hanson, M.A., Powell, H.C., Barth, A.T., Ringgenberg, K., Calhoun, B.H., Aylor, J.H., Lach, J.: Body area sensor networks: Challenges and opportunities. Computer 42(1), 58–65 (2009)
11. Curtis, D.W., Pino, E.J., Bailey, J.M., Shih, E.I., Waterman, J., Vinterbo, S.A., Stair, T.O., Guttag, J.V., Greenes, R.A., Ohno-Machado, L.: SMART–An Integrated Wireless System for Monitoring Unattended Patients. Journal of the American Medical Informatics Association, 44–53 (2008)
12. Ko, J., Lim, J.H., Chen, Y., Musvaloiu-E, R., Terzis, A., Masson, G.M., Gao, T., Destler, W., Selavo, L. Dutton, R.P.: MEDiSN: Medical emergency detection in sensor networks. In: Proc. ACM Transactions on Embedded Computing Systems, pp. 11:1–11:29. ACM, New York (2010)
13. Chipara, O., Lu, C., Bailey, T.C., Roman, G.-C.: Reliable clinical monitoring using wireless sensor networks: experiences in a step-down hospital unit. In: Proc. 8th ACM Conference on Embedded Networked Sensor Systems, Switzerland, pp. 155–168. ACM, New York (2010)
14. Sharma, S., Vyas, A.L., Thakker, B., Mulvaney, D., Datta, S.: Wireless Body Area Network for health monitoring. In: Proc. 4th International Conference on Biomedical Engineering and Informatics, Shanghai, pp. 11:2183–11:2186. ACM, New York (2011)
15. Chang, Y.-J., Chen, C.-H., Huang, W.-T., Chen, Y.-Y., Kuo, C.-Y.: A Data-Driven Architecture for Remote Control of Sensors over a Wireless Sensor Network and the Internet. In: Proc. 10th International Symposium on Pervasive Systems, Algorithms, and Networks, Kaohsiung, pp. 11:344–11:349. IEEE Press, New York (2009)
16. Hamida, E.B., D'Errico, R., Denis, B.: Topology Dynamics and Network Architecture Performance in Wireless Body Sensor Networks. In: Proc. 4th IFIP International Conference on New Technologies, Mobility and Security, Istanbul, pp. 11:1–11:6. IEEE Press, New York (2011)
17. Ge, Y., Liang, L., Ni, W., Wai, A.A.P., Feng, G.: A measurement study and implication for architecture design in wireless body area networks. In: Proc. IEEE International Conference on Pervasive Computing and Communications Workshops, Lugano, pp. 799–804. IEEE Press, New York (2012)
18. Abousharkh, M., Mouftah, H.: Service oriented architecture-based framework for WBAN-enabled patient monitoring system. In: Proc. Second Kuwait Conference on e-Services and e-Systems, Kuwait, pp. 18:1–18:4. ACM, New York (2011)
19. Gui-Ling, S., Jia-Long, Y.U., Ying, Z., Wei-Xiang, L.I.: Design and implementation of sensor nodes for a Wireless Body Area Network. In: Proc. 4th International Conference on Biomedical Engineering and Informatics, Shanghai, pp. 1403–1406. IEEE Press, New York (2011)

20. Omeni, O.C., Eljamaly, O., Burdett, A.J.: Energy Efficient Medium Access Protocol for Wireless Medical Body Area Sensor Networks. In: Proc. 4th IEEE/EMBS International Summer School and Symposium on Medical Devices and Biosensors, Cambridge, pp. 29–32. IEEE Press, New York (2007)
21. Kwon, H., Lee, H.: Energy-efficient multi-hop transmission in Body Area Networks. In: Proc. 20th International Symposium on Personal, Indoor and Mobile Radio Communications, Tokyo, pp. 2142–2146. IEEE Press, New York (2009)
22. Ameen, M.A., Ullah, N., Chowdhury, C.S., Islam, S.M.R., Kwak, K.: A power efficient MAC protocol for wireless body area networks. EURASIP Journal on Wireless Communications and Networking (2012)
23. Timmons, N.F., Scanlon, W.G.: An Adaptive Energy Efficient MAC Protocol for the Medical Body Area Network. In: Proc. 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, Aalborg, pp. 587–593. IEEE Press, New York (2009)
24. Chipara, O., Brooks, C., Bhattacharya, S., Lu, C., Chamberlain, R.D., Roman, G.-C., Bailey, T.C.: Reliable Real-time Clinical Monitoring Using Sensor Network Technology. In: Proc. AMIA Annual Symposium, San Francisco, pp. 103–107 (2009)
25. Arrobo, G.E., Gitlin, R.D.: Improving the reliability of wireless body area networks. In: Proc. 33rd Annual International Conference of the IEEE on Engineering in Medicine and Biology Society, Boston, pp. 2192–2195. IEEE Press, New York (2011)
26. Ivanov, S., Botvich, D., Balasubramaniam, S.: Cooperative wireless sensor environments supporting body area networks. Proc. IEEE Transactions on Consumer Electronics, 1230–1234 (2012)
27. Sampangi, R.V., Urs, S.R., Sampalli, S.: A novel reliability scheme employing multiple sink nodes for Wireless Body Area Networks. In: Proc. Symposium on Wireless Technology and Applications, Malaysia, pp. 162–167. IEEE Press, New York (2011)
28. Yun, D., Kang, J., Kim, J.-E., Kin, D.: A Body Sensor Network Platform with Two-Level Communications. In: Proc. International Symposium on Consumer Electronics, Irving, pp. 1–6. IEEE Press, New York (2007)
29. Ivanov, S., Foley, C., Balasubramaniam, S., Botvich, D.: Virtual Groups for Patient WBAN Monitoring in Medical Environments. Proc. Transactions on Biomedical Engineering, 3238–3246 (2012)
30. Debdhanit, Y., Joseph, K.: Continuous vs. Event Driven Routing Protocols for WSNs in Health-care Environments. In: Pervasive Health Conference and Workshops, pp. 1–4. IEEE Press, New York (2006)
31. Kwon, H.C., Na, D., Ko, B.G., Lee, S.: An energy-efficient communication method based on the relationships between biological signals for ubiquitous health monitoring. In: Proc. 30th Annual International Conference IEEE on Engineering in Medicine and Biology Society, Vancouver, pp. 1541–1544. IEEE Press, New York (2008)
32. Ababneh, N., Timmons, N., Morrison, J.: EBRAR: Energy-balanced rate allocation and routing protocol for body area networks. In: Proc. Symposium on Computers and Communications, Cappadocia, pp. 000475–000478. IEEE Press, New York (2012)
33. Manfredi, S.: Reliable and energy-efficient cooperative routing algorithm for wireless monitoring systems. In: Proc. IET on Wireless Sensor Systems, pp. 128–135. IEEE Press, New York (2012)

34. Quwaider, M., Biswas, S.: On-body Packet Routing Algorithms for Body Sensor Networks. In: Proc. First International Conference on Networks and Communications, Chennai, pp. 171–177. IEEE Press, New York (2009)
35. Ho, Q.-D., Tran, T.-N., Rajalingham, G., Le-Ngoc, T.: A distributed and adaptive routing protocol designed for wireless sensor networks deployed in clinical environments. In: Proc. Wireless Communications and Networking Conference, Paris, pp. 2746–2750. IEEE Press, New York (2012)
36. Liang, X., Li, X., Shen, Q., Lu, R., Lin, X., Shen, X., Zhuang, W.: Exploiting prediction to enable Secure and Reliable routing in Wireless Body Area Networks. In: Proc. INFOCOM, Orlando, pp. 388–396. IEEE Press, New York (2012)

Assessing Data Reliability in Mobile Wireless Sensor Network*

Rabail Kazi, Nafeesa Bohra, and Faisal Karim Shaikh

Department of Telecommunication, Mehran University of Engineering
and Technology Jamshoro, Pakistan
76062, Jamshoro, Pakistan
rabail.kazi08tl54@student.muet.edu.pk,
{nafeesa.zaki,faisal.shaikh}@faculty.muet.edu.pk
http://www.tl.muet.edu.pk

Abstract. Mobility in Wireless Sensor Networks (WSNs) introduces significant challenges which do not arise in static WSNs. Reliable data transport is an important aspect of attaining consistency and Quality of Service in several applications of Mobile Wireless Sensor Networks (MWSNs). It is important to understand how each of the wireless sensor networking characteristics affects reliability. If reliability is not managed well, the MWSN can suffer from overhead and hence its applicability in the real world would be affected. In this research, the main emphasis is given to reliability assessment and is being studied by deploying MWSN in different indoor and outdoor scenarios. Results show that the reliability is greatly affected when mobile mote sends data to the neighboring static motes using inherent mechanism used by TinyOS.

Keywords: Wireless Sensor Network, Mobile WSN, Reliability, Mica2, Mobility.

1 Introduction

The traditional WSN architecture consists of a large number of static sensor motes which are densely deployed over an area of interest. Sensor motes are tiny, battery-operated computing devices operational with sensors capable of sensing information from their surroundings. Sensor motes collect data from their surroundings, process them locally and send the results to a data collecting point, usually a base station mote. Initially WSNs were deployed in a hostile environment for military surveillance in order to collect information about the opponent actions. Later on, due to WSN applicability, it become a convenient tool for environmental monitoring [1], utility metering [2] and many other applications [3]. Additionally, the cost for processing power and wireless communication started to decrease which eventually made WSNs more reasonable and more

* This research was partially supported by Mehran University of Engineering and Technology, Jamshoro, Pakistan and National ICT R&D Fund, Ministry of Information Technology, Pakistan under National Grassroots ICT Research Initiative.

F.K. Shaikh et al. (Eds.): WSN4DC 2013, CCIS 366, pp. 73–84, 2013.

attractive [4]. Generally, the radio range of sensor motes is less and the communication paradigm between the sensors motes and the data collection point is multi-hop. WSNs often do not work as anticipated when deployed in the real world due to many reasons. For example, environmental influence can result a non-deterministic performance of sensor motes. Similarly, radio communication may affect the overall performance of data transfer or even malfunctioning of the sensor mote may happen. In addition to the above mentioned facts, reliability of the data transport is compromised by interference and collisions because of the multihop communication paradigm. As a result, the number of message drop increases with the number of hops and hence reliability becomes the major concern.

The traffic pattern inherent to WSNs is convergecast, i.e., messages generated from the sensor motes are collected by the base station mote. As a consequence, motes closer to the base station mote are more overloaded than others, and subject to premature energy depletion. This issue is known as the funneling effect [5]. In order to solve the problem mentioned above, large number of motes need to be deployed. Increasing the number of motes will not only increase the cost of the network but since the motes near base station are overloaded, therefore data may not be transported. The failures relevant to the data transport include message loss and higher message delays. These failures directly impact the responsiveness of the WSNs. The problems mentioned above can be improved by introducing the mobility in WSNs. Instead of collecting data through Multihop, the mobile motes can visit static motes in the network and collect/send data directly through single-hop transmission. This will not only reduce the contention and collisions, but will also reduce the message loss. Single-hop transmission also help in reducing the funneling effect, as mobile motes can visit different regions in the network and spread the energy consumption more uniformly even in the case of a dense WSN architecture. Generally, the MWSNs can be adapted easily for delay-tolerant applications [6]. Mobility can also be exploited in scenarios where motes are attached to mobile objects, in many cases animals, for examples zebras [7] or rats [8]. Such applications often use delay-tolerant networking approaches since there is no need for real-time data and since the network is usually sparse and mobile encounters are rare events. Mobility in WSNs introduces significant challenges which do not arise in static WSNs. Some of the major challenges are contact detection, reliable data transfer, and mobility control.

- *Contact detection:* Since communication is possible only when the motes are in the transmission range of each other, it is necessary to detect the presence of a mobile mote correctly and efficiently. This is especially true when the duration of contacts is short.
- *Reliable data transfer:* As available contacts might be scarce and short, there is a need to maximize the number of messages correctly transferred to the sink. In addition, since motes move during data transfer, message exchange must be mobility-aware.

- *Mobility control:* When the motion of mobile motes can be controlled, a policy for visiting motes in the network has to be defined. To this end, the path and the speed or sojourn time of mobile motes have to be defined in order to improve (maximize) the network performance

Apart from the issues mentioned above another major issue with WSNs is of reconfiguration. As after deploying the WSN some or all of the static motes need reconfiguration. Generally, the base-station mote broadcast new parameters and configuration updates to its neighbor motes. In response to that the neighbor motes further broadcast the reconfiguration messages to their neighbors and by this way all motes or subset of motes are updated. This process of updating the network require lot of messages to be exchanged across the network. In order to encounter this problem, the mobile motes can be programmed in such a way that it sends the new parameters only to those static mote where it is mandatory hence reducing the overhead.

The work presented in this research is solemnly based on assessing data reliability in MWSN. It is crucial to evaluate the factors due to which the number of messages are correctly transferred between mobile and static motes.

The remainder of the paper is organized as follows. Section 2 proceeds with the related work followed by methodology and experimental environments used for assessing the data reliability in Section 3. Section 4 presents the results while Section 5 concludes the paper.

2 Related Work

The study of reliable data transport in WSNs has been the subject of extensive research during the last decade [9],[10],[11],[12],[13],[14],[15],[16],[17]. More recently mobility has also been introduced to WSNs. In fact, mobility in WSNs is useful for several reasons e.g. cost, connectivity, reliability and energy efficiency [18] ,[19]. Nowadays, testbeds are even created for the support of mobility in WSN e.g. [20]. In [20] the authors present Sensei-UU, a sensor network testbed which supports mobile sensor motes. Since, there are many issues (e.g. localization, energy-efficiency, contact detection) which can be addressed by exploiting mobility in WSNs. Still, limited body of work exists for assessing the data reliability in MWSN. The reliability issue in MWSNs is presented in [21]. The authors in [21] presented a system for data collection from sparse sensor networks with the help of mobile relays. The authors in [22] proposed a message ferrying approach for data delivery in sparse mobile Ad hoc networks. In [19] authors have provided an extensive survey by giving a comprehensive taxonomy of MWSN architectures and as well as presented an overview of the data collection process. In [23], the authors have demonstrated the data collection from mobile motes in scenarios where all motes, both base station and sources, are mobile.

The above approaches are limited in the sense that they are only considering the collection of data from the static sensor motes. They do not consider other actions such as reconfiguring the parameters of the static motes with the help of mobile mote without causing the entire network to be disturbed.

From the above discussion it is concluded that there is a need for assessing the data reliability in MWSN when particularly the mobile mote transfers the data or the parameters to the static motes.

3 Methodology and Experimental Environment

3.1 Methodology

Experiments are carried out by setting up a test bed of 8 Mica2 motes with the TinyOS operating system [23], and laptops running Windows XP equipped with MIB510 serving as the base-station. Various indoor and outdoor experiments were performed. In order to improve the measurement precision of Mica2 motes a system called virtual ground is used. In virtual ground, each Mica2 mote has a small plastic cup below it so that the antenna sees an equipotential surface as floor, and it acts like a dipole because of reflections. When utilizing the virtual ground, the transmission channel is further consistent because it limits the occurrence of reflection and bad electromagnetic waves perturbation. In [24], the authors have investigated the performance of Mica2 motes by means of an extensive experimental analysis. They carried out various experiments and found that for Mica2 mote the transmission range is 70 m with the maximum transmission power of 5 dbm.

Initially, the code was executed under the TOSSIM environment [25] (a simulation environment to examine NesC programs), and after an extensive testing, programs were compiled and installed on the Mica2 motes. For the experimental tests, the modified Surge application was flashed onto the Mica2 motes, giving each mote a unique ID. In order to retrieve the data base-station mote was linked with the computer through the serial port. The MIB510 is a programming board that acts as base station for the Mica2 motes. Through the sinks NesC compiled programs can be flashed to the motes and data can be uploaded or retrieved from or to the motes. For the experiments a base station mote was programmed to a mote with Id 0. The base station mote retrieves the transferred data and processes it with a Java application which includes one mote (base station) connected to a PC running cygwin. The mote with ID 10 is the mobile mote. A tiny packet generator was developed to send messages at regular intervals to the static motes (motes with IDs other than 0 and 10). The other 6 motes (static motes) are also programmed in such a way that they show the number of messages received by the mobile mote to the base station. The results were observed by the number of messages received by the static mote in the topology visualizer. Several experiments have been performed in order to assess the reliability

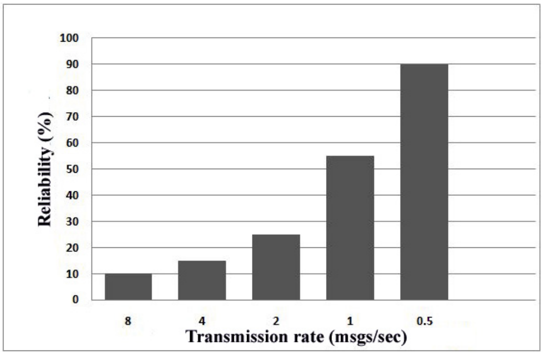


Fig. 1. Reliability v/s transmission rate

by observing the message loss scenario. The performance is measured in terms of total number of messages successfully transferred against the total number of messages successfully received by the static sensor motes.

To ensure that the messages are successfully transferred from mobile mote to static mote, the timer rate was adjusted precisely to avoid any unwanted losses. Initial experiments are carried indoor where a single static and mobile motes are taken into account. One static mote with ID 1 was placed at a distance of 5m from the base station mote (ID 0), whereas the mobile mote (ID 10) was placed at a distance of 10m from the static mote, in static position. 20 mobile messages from mobile mote to static mote at different mobile timer rates, starting from 8 msgs/sec to 0.5 msgs/sec, provided that the initial timer rate for the static mote remains constant (0.5 msgs/sec). The achieved reliability is shown in Fig. 1. It is analyzed from Fig. 1 that in order to achieve at least 90% reliability the mobile timer rate should be equal to or less than 0.5 msgs/sec.

For all experiments the Tiny OS parameter values are summarized in Table 1.

Table 1. Parameter Values used for Mica2 motes

Frequency	916 MHZ
Data rate	19.2 kbps
Power	0 dB/mW (10.4mA)
Duty Cycle	100%
Antenna position	Back to back

3.2 Experimental Environment

Experiments have been performed indoor and outdoor at the premises of the Dept. of Telecommunication Engg. Mehran UET, Jamshoro. Indoor experiments have been performed inside the corridors so as to create a sub-urban scenario (because during the tests students happened to pass by and between motes). For outdoor experiments the parking area has been used in order to create a realistic urban scenario (because during the tests cars happened to pass by and between motes). The communication model discussed above is straightforward and systematically tractable. Yet, it is not entirely realistic for the following reasons. First, the transmission range is not perfectly circular because the wireless medium is non-isotropic. Secondly, the packet loss experienced by the mobile mote does not drop immediately to zero as soon as the mobile mote enters the static motes radio range. It progressively tends to zero as the mobile mote approaches the static one. Moreover, it does not exhibit a regular behavior. It may happen that the packet loss increases temporarily even if the distance between motes decreases.

Alg. 1, Alg. 2, and Alg. 3 describes the our approach for accessing the reliability which is a modified version of Surge application of Tiny OS. The Surge application is basically a simple example of a WSN multihop application. Surge takes sensor readings and sends them towards the base mote (mote with ID 0). Accompanying this application is a Java program that can be used to visualize the logical network topology and the sensor readings. Main features of the Surge application includes the detection of the existence of all the motes in WSN, displays mote information; including the mote identification number (ID), the number of messages sent from each mote and displays the topology of network. Surge after modification can be used for both WSN and MWSN. The Surge features are enhanced, e.g., it also shows the number of mobile messages received by the static motes from the mobile mote. Hence, the impact of adding mobility to a WSN can now be viewed considerably.

Algorithm 1. For Mobile Mote

```
if ID == MOBILE_ID then
    send mobile_message();
    call Leds.greenOn();
    //signals that we are sending a new message
    counter++;
    call Leds.greenOff();
    //signals that we sent a new message
end
```

Algorithm 2. For Static Motes

```
if ID != MOBILE_ID and ID != BASE_STATION then
    receive mobile_message();
    call Leds.redOn();
    //signals that we are receiving a new message
    counter++;
    send to_BaseStation(counter);
    //send to mote ID 0
    call Leds.redOff();
    //signals that we received a new message
end
```

Algorithm 3. For Base Station Mote

```
if $ID == BASE\_STATION$ then
    receive keep_alive(ID);
    receive(counter);
    //Number of mobile message received at all static motes
    show(counter);
    //at Java topology visualizer
end
```

The analysis is divided into two main parts, i.e., indoor and outdoor. First, indoor scenarios are considered and the reliability is assessed by initially keeping the mobile mote static (0 m/s) and then moving at a normal pedestrian speed (0.625 m/s). The second part consists of the outdoor scenario where at first the mobile mote is kept static (0 m/s) and then moving faster than the normal pedestrian speed (1.25 m/s).

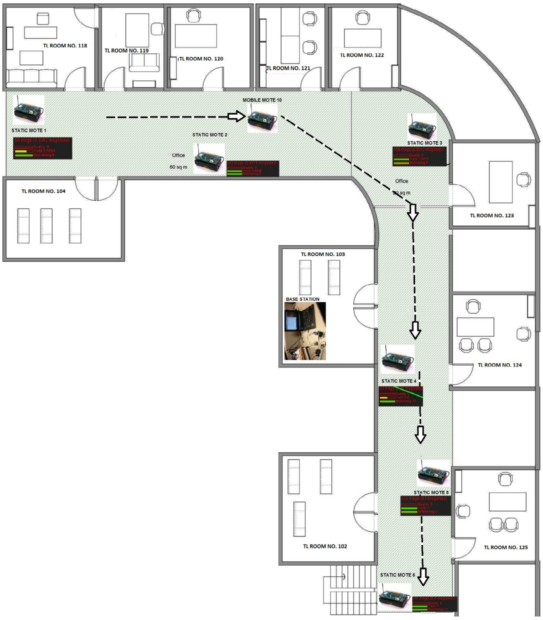


Fig. 2. Indoor experiment with 6 static motes, one base station and one mobile mote moving at a constant rate

Fig. 2 shows the indoor environment, where 6 static motes with IDs 1, 2, 3, 4, 5 and 6 are placed at a distance of 5 meters from one another at the ground floor of Dept. of Telecommunication. One base-station mote with ID 0 is connected to laptop through programming board inside the Project Lab whereas the Mobile mote is having ID 10.

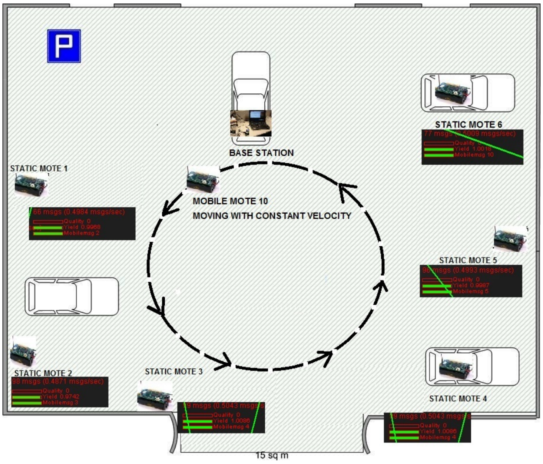


Fig. 3. Scenario of outdoor experiment with 6 static motes, one base station and one mobile mote moving at a constant rate

Fig. 3 explains the outdoor environment with 6 static motes with IDs 1, 2, 3, 4, 5 and 6 placed at a distance of 10 meters from one another in the parking area of the Dept. of Telecommunication. The static motes with ID 4 and 6 were placed on the roof of the cars while others were placed on the virtual ground system. One base station mote with ID 0 is connected to laptop through programming board and is placed on the roof of a car. One mobile mote with ID 10 is placed in the center location of all the static motes.

4 Experimental Results

This section comprises of the results observed from various experiments based on different indoor and outdoor scenarios.

4.1 Indoor Scenario

Initially the mobile mote with Id 10 is placed in between mote 3 and mote 4 in static position. After the setup, 20 mobile messages were sent from mobile mote to static motes with a constant rate of 0.5 msgs/sec.

It is analyzed from the results shown in Fig. 4, that the static mote 3 is up to 95% reliable and static mote 4 is about 85% reliable because the static mote 3 gets 19 messages and static mote 4 gets 17 messages out of 20 messages sent from mobile mote. The reason behind this is that when the mobile mote is in static position only the motes near to it will receive messages and due to the presence of obstacles like walls, and ground reflections, the other motes are unable to receive the messages from mobile mote.

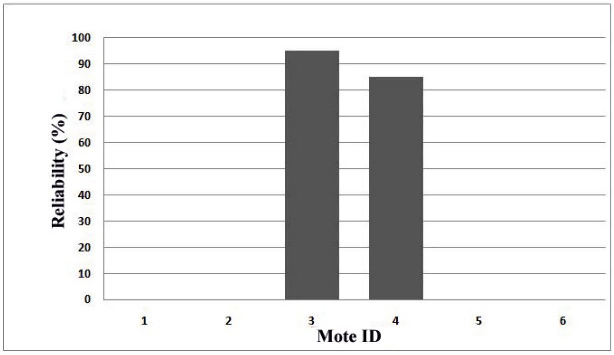


Fig. 4. Reliability for static indoor scenario

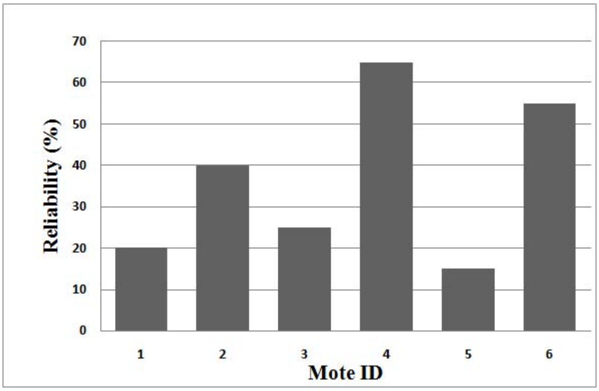


Fig. 5. Reliability for mobile indoor scenario

Fig. 5 shows the analysis where the mobile mote with ID 10 is moving with a constant velocity of 1.25 m/sec from static mote ID 1 to static mote ID 6. Again 20 messages were sent from the mobile mote to the static mote with a constant rate of 0.5 msgs/sec. It is analyzed that the static mote 1,2,3,4,5,and 6 achieve 20%, 40%, 25%, 65%, 15%, and 55% reliability respectively. From the above analysis it is observed that as soon as the mobile mote gets closer to the static mote, the static motes receives the mobile messages but still motes with Id. No: 4 and 6 gets more reliability than the others. This is because the presence of some students was observed, while mobile mote was moved, hence, the reliability on the other motes decreases. In order to achieve reliability the deployment of the network (indoor) must be done at some height from the ground and the static motes should be placed in such a way to avoid obstructions, and reflections strength is experienced to be at its maximum.

4.2 Outdoor Scenario

After the setup, 20 mobile messages were sent from mobile mote to the static motes with a constant rate of 0.5 msgs/sec.

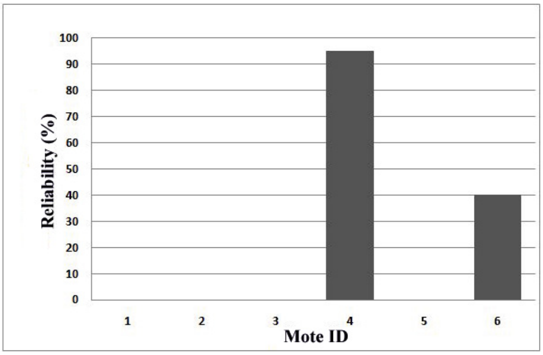


Fig. 6. Reliability for static outdoor scenario

Fig. 6 shows that the static mote 4 achieves up to 95% reliability while the static mote 6 achieves 40% reliability. The other motes did not receive any messages sent by the mobile mote, because the motes 4 and 6 were placed on the car's roof, i.e. at some height from the ground and also the mobile mote was placed at 5 meter above the ground while the other motes were placed on the ground. This is the reason that they were not able to receive any mobile message.

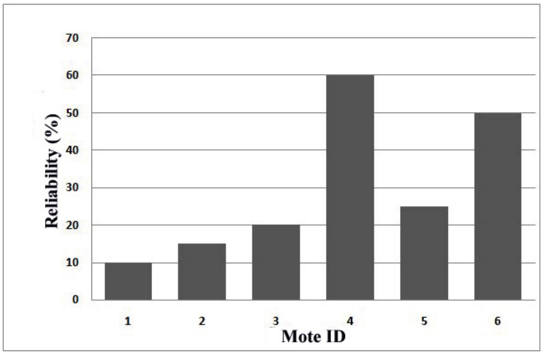


Fig. 7. Reliability for mobile outdoor scenario

Fig. 7 shows the analysis where the mobile mote with ID 10 is moved with a constant velocity of 1.25 m/sec from static mote 1 to the static mote 6. Again 20 mobile messages were sent from the mobile mote to static motes at a constant rate of 0.5 msgs/sec.

It is observed that the static mote 1, 2, 3, 4, 5, and 6 achieve 10%,15%, 20%, 60%, 25%, and 50% reliability. It is again observed that static motes 4 and 6 are the most reliable of all because these motes were placed on the cars, i.e., on some height from the ground. Apart from this the mobile mote was also moved on some height above from the ground while the other motes were placed on the virtual ground and hence they were receiving less number of mobile messages.

In order to make the other motes more reliable these motes must be placed at some height from the ground.

5 Conclusion

The main objective of this research is to assess how reliably the mobile mote transfers data when it is moving with a constant velocity. Overall we observe that due to mobility there is a loss of packets and 100% reliability is not achieved by existing protocol. We observe that reliability is bit higher in indoor environment compared to that of outdoor environment. There is need to carefully analyze how the reliability can be increased by adopting appropriate acknowledgment mechanisms in order to retrieve the lost packets.

References

1. Khelil, A., Shaikh, F., Ali, A., Suri, N.: gMAP: an efficient construction of global maps for mobility-assisted wireless sensor networks. In: Proceedings of the Conference on Wireless on Demand Network Systems and Services, WONS, pp. 189–196 (2009)
2. Hill, J.L.: System architecture for wireless sensor networks. Ph.D. dissertation, University of California, Berkeley, California, United States (2003)
3. Kuorilehto, M., Hännikäinen, M., Hämäläinen, T.D.: A survey of application distribution in wireless sensor networks. EURASIP J. Wirel. Commun. Netw. 2005(5), 774–788 (2005)
4. Yan, T.: Analysis approaches for predicting performance of wireless sensor networks. Ph.D. dissertation, University of Virginia (2004)
5. Li, J., Mohapatra, P.: Analytical modeling and mitigation techniques for the energy hole problem in sensor networks. Pervasive Mobile Computing 3 (June 2007)
6. Voyiatzis, A.: A survey of delay- and disruption-tolerant networking applications. Journal of Internet Engineering 5(1), 331–344 (2012)
7. Liu, T., Sadler, C., Zhang, P., Martonosi, M.: Implementing software on resource-constrained mobile sensors: Experiences with impala and zebranet. In: Proceedings of the 2nd International Conference on Mobile Systems, Applications, and Services, pp. 256–269 (2004)
8. Link, J.A.B., Wehrle, K., Osechas, O., Thiele, J.: Ratpack: Communication in a sparse dynamic network. In: ACM SIGCOMM (2008)
9. Akyildiz, I., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless sensor networks: a survey. Computer Networks 38(4), 393–422 (2002)
10. Sankarasubramaniam, Y., Akan, O.B., Akyildiz, I.F.: Esrt: event-to-sink reliable transport in wireless sensor networks. In: International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc (2003)
11. Stann, F., HeIdemann, J.: Rmst: Reliable data transport in sensor networks. In: International Workshop on Sensor Network Protocols and Applications, SNPA, pp. 102–112 (2003)
12. Stathopoulos, J., HeIdemann, T., Estrin, D.: A remote code update mechanism for wireless sensor networks. University of California, Los Angeles. Technical Report CENS-TR-30 (2003)

13. Texan, N., Cayirci, E., Caglayan, M.U.: End-to-end reliable event transfer in wireless sensor networks. In: Personal Indoor and Mobile Radio Communications, PIMRC, vol. 2, pp. 989–994 (2004)
14. Wan, C., Campbell, A.T., Krishnamurthy, L.: Psfq: a reliable transport protocol for wireless sensor networks. In: International Workshop on Wireless Sensor Networks and Applications, WSNA, pp. 1–11 (2002)
15. Wang, C., Daneshmand, M., Li, B., Sohraby, K.: A survey of transport protocols for wireless sensor networks. IEEE Network Magazine (2006)
16. Zhang, H., Arora, A., Choi, Y., Gouda, M.G.: Reliable bursty convergecast in wireless sensor networks. In: Interational Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc, pp. 266–276 (2005)
17. Zhou, Y., Lyu, M.R.: Port: A price-oriented reliable transport protocol for wireless sensor networks. In: International Symposium on Software Reliability Engineering, ISSRE, pp. 117–126 (2006)
18. Anastasi, G., Conti, M., Di, F.: G. anastasi, m. conti, m. di francesco, an analytical study of reliable and energy-efficient data collection in sparse sensor networks with mobile elements. In: Proceedings of EWSN (2006)
19. Di Francesco, M., Das, S., Anastasi, G.: Data collection in wireless sensor networks with mobile elements: A survey. ACM Transactions on Sensor Networks (2011)
20. Rensfelt, O., Hermans, F., Gunningberg, P., Åke Larzon, L.: Repeatable experiments with mobile nodes in a relocatable wsn testbed. In: The First International Workshop on Mobility in Wireless Sensor Networks, MobiSensor 2010 (2010)
21. Anastasi, G., Conti, M., Di Francesco, M.: Reliable and energy-efficient data collection in sparse sensor networks with mobile elements. Perform. Eval. 66(12), 791–810 (2009)
22. Zhao, W., Ammar, M., Zegura, E.: A message ferrying approach for data delivery in sparse mobile ad hoc networks. In: Proceedings of the 5th ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc 2004, pp. 187–198 (2004)
23. Navid, H., Olaf, L., Frederik, H., Olof, R., Thiemo, V.: Efficient mobile data collection with mobile collect. In: The 8th IEEE International Conference on Distributed Computing in Sensor Systems, DCOSS (2012)
24. Anastasi, G., Falchi, A., Passarella, A., Conti, M., Gregori, E.: Performance measurements of motes sensor networks. In: Proceedings of the 7th ACM International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems, MSWiM 2004, pp. 174–181 (October 2004)
25. Levis, P., Lee, N., Welsh, M., Culle, D.: Tossim: Accurate and scalable simulation of entire tinyos applications. In: Proceedings of the First ACM Conference on Embedded Networked Sensor Systems, SenSys, Los Angeles, CA, USA (2003)

Simultaneously Node Relocation Algorithm for Mobile Sensor Network

Muhammad Amir Khan[1], Halabi Hasbullah[1], Babar Nazir[2],
Imran Ali Qureshi[3], and Nasrullah Pirzada[1,3]

[1] Computer and Information Science department, Universiti Teknologi PETRONAS, Malaysia
{Amirkhancomsats,nasrullahpirzada}@gmail.com,
halabi@petronas.com.my
[2] Department of Computer Science, COMSATS Institute of IT Abbottabad Pakistan
babarnazir@gmail.com
[3] Department of Telecommunication Engineering
Mehran University of Engineering and Technology Jamshoro Pakistan
i.ali1225@yahoo.com

Abstract. For collecting valuable data in Mobile sensor network, the inter-sensor connectivity plays a vital role. Nodes in these networks monitor different regions of an area of interest. In which failure of a sensor node can leads to loss of connectivity and may cause partitioning of the network into disjoint segments. A number of approaches that pursue node relocation to restore connectivity have recently been proposed. However, these approaches tend to ignore the possible loss of coverage in some areas, either due to the failure itself or due to the connectivity-limited focus of the recovery. This paper fills this gap by addressing the connectivity and coverage concerns in an integrated manner. A novel simultaneously node repositioning algorithm is presented. Each neighbor temporarily relocates to substitute the failed node, one at a time, and then returns back to its original location. The algorithm is validated using the performance parameter, distance moved and it is worth noting that our algorithm handles well the increase in network connectivity.

Keywords: Wireless Sensor Networks (WSN), node relocation, failure recovery, mobile sensors, network connectivity.

1 Introduction

As one of the most significant technologies, Wireless Sensor Networks (WSN), for its wide utility at recent comes to be a well-developed research field. Commonly, a WSN will comprise a large number of compactly installed small mobile sensor nodes, which have a low power and affordable cost. Again, it is mostly successfully applied for the environment observation, data processing and communication between each other through radio [1-5]. Not only can WSN decrease the cost and delay in development, but also it can be applied into any environment, particularly those in which conventional wired sensor network are impossible to be deployed like in the deep oceans, outer space or battle field [6, 7]. Sensor nodes are also mostly used in health,

F.K. Shaikh et al. (Eds.): WSN4DC 2013, CCIS 366, pp. 85–95, 2013.

home or military. Due to their prompt operation, self-organization, and fault tolerance individuality, sensor networks in military for example become highly suitable for any armed forces systems such as for commanding, controlling, communication, surveillance and also targeting. Sensor nodes in health on the other hand are to be applied in monitoring patient and helping disabled patients. They could moreover be applicable in other commercial matters such as managing inventory, and monitoring product quality and disaster areas as well [8-10].

Fig. 1 illustrates the deployed sensor nodes randomly presented in a sensor field; each of which carries out the previously assigned task and communicates each other in directing sensing data back to the sink such as the communication link among sensor nodes 1, 2, 3, 4, and 5. Once obtained in the form of useful information, the data subsequently are addressed to the user through internet [11].

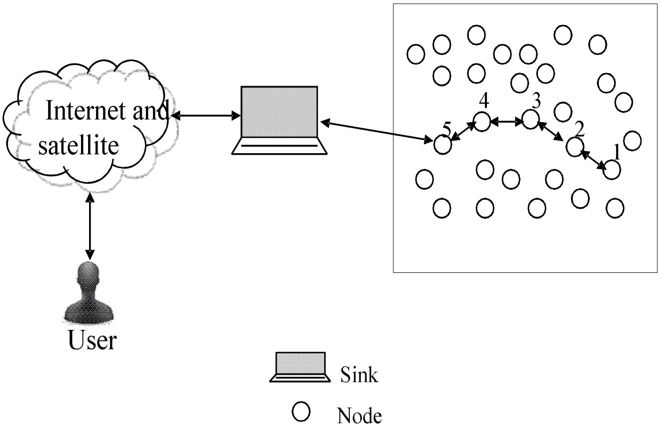


Fig. 1. Randomly scattered Wireless Sensor Network (WSN)

For deployment in harsh and unattended areas a node loss can be encountered because of the depletion of onboard energy or a physical damage causing the network to likely be separated into multiple disjoint blocks and thus stop working [12-15]. Therefore, dynamically repositioning the nodes while the network is operational is necessary to further improve the performance of the network. For instance, when many of the sensors in the vicinity of the base-station stop functional due to the exhaustion of their batteries, some redundant sensors from other parts of the monitored region can be identified and relocated to replace the dead sensors in order to improve the network lifetime. Such dynamic relocation can also be very beneficial in a target tracking application where the target is mobile. For instance, some of the sensors can be relocated close to the target to increase the fidelity of the sensor's data. Moreover, in some applications it may be wise to keep the base-station a safe distance from harmful targets, e.g., an enemy tank, by relocating it to safer areas in order to ensure its availability [16]. Not only is the inter-node connectivity very critical for the application effectiveness, but also some nodes might play a role in maintaining the flow of information from the sensors in place and the remote users [17]. Deploying a substitution of the futile node could be taking a lot of time and frequently being impossible in unsafe situation such as in battle. Some studies have informed that the node repositioning has been deemed to be an efficient way in restoring partitioned networks. However, these previous studies are more concerned with the restoration of the missing connectivity without any considerations for the unconstructive impact of relocation of nodes on coverage such as in relocating the redundant node in place of failure node [18-19]. According to [20, 21] coverage with good connectivity can also be used as a measure of the QoS of the sensor network. It then seems that coverage and connectivity have to be considered side by side. A previously work has shown that a single node failure without any additional redundant node in the network is comparable to baseline approaches [22]. This paper contributes to filling such a research gap and proposes a simultaneously node repositioning algorithm. Unlike other approaches that readjust the network topology by repositioning nodes, the proposed algorithm strives to keep most of the network topology intact and localize the scope of recovery. Basically, the failure of a node is tolerated by temporarily replacing it with one of its neighbors. These neighbors take turns in moving to the position of the failed node. Upon detecting the failure, neighbors nodes coordinate to establish a schedule for each of them to reposition toward the failure node. After serving for some time, a node will go back to its original position, allowing for other neighbor of failed node to come forward and so on. Our algorithm is a distributed algorithm and requires very limited messaging overhead in conducting the recovery.

2 Literature Review

Node relocation problem is well-studied [23]. Some approaches allow movement only between initial deployment and application startup (post-deployment), while others can arrange movement at any time (on-demand).

2.1 Post-deployment Repositioning

For the reposition of post-deployment, three related algorithms have been recommended by Wang et al. [24], namely VOR, VEC, and Minimax, Each of which concerns with a sensor node's Voronoi polygon, the closest node as the part of the sensing area. VEC goes behind Coulomb's law, an equation illustrating how electrostatic particles prevent each other. Once a part of a node's Voronoi polygon is not covered, the node will be repelled from its neighbors by a force proportional to its distance either from them or from the vertices of the polygon. Heo and Varshney [25] proposed an equivalent method as a reflection of Coulomb's law, yet not considering the node's Voronoi polygon. As a substitute, each node will then proportionally move in a distance to the density of nodes in its immediate area. VOR merely causes the node to move toward the most distant vertex of its Voronoi polygon, leading the polygons to be more regular. VOR however tends to lead the nodes to fluctuate between multiple locations. The Minimax algorithm could emerge the shorter, more conventional movement and also less fluctuation. All three algorithms then lead the motion irregular, thus becoming inefficient in energy and time.

A proxy-based approach in order to abbreviate the total travel distance is proposed in [26] in which the sensor nodes do not physically move - except their destination is already calculated. The authors more emphasize on a network supported by stationary and mobile sensors. Mobile sensors here are to fill coverage holes distributively recognized by stationary nodes. Hence, they only logically move and designate the stationary sensor nodes as their proxies. The total and averaged distance passed through mobile nodes while maintaining the same level of coverage as [24] are much decreased by this approach – only for the message complexity does this approach increase. These approaches after all are more emphasized on evading holes in coverage than maintaining connectivity.

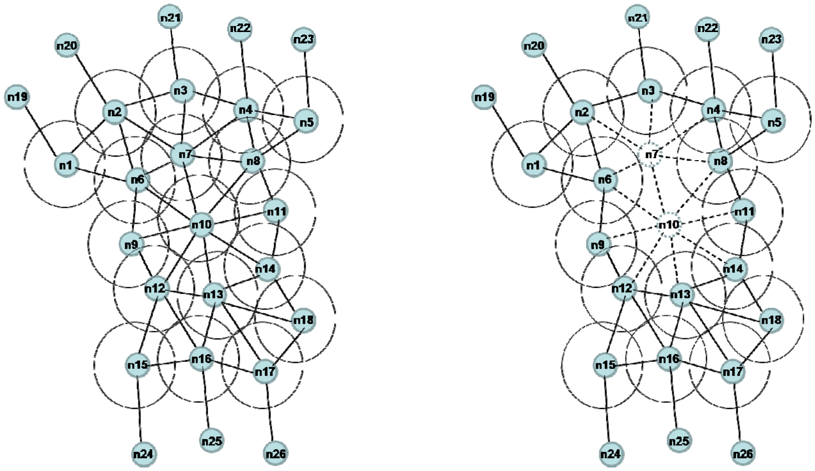
2.2 On-Demand Repositioning

Placing into the most efficient structure is becoming the goal of the mentioned algorithm. At the starting of network application, efficiency largely might be lessened by the failure of the node, and changes in application requirements may additionally effect on the meaning of efficiency itself. Nodes in either case are supposed to move in order to keep efficiency of a network layout. To substitute a failed sensor, Cascaded Movement has been proposed by Wang et al [27] by iteratively replacing a nearby node with a redundant node. Also, other works have considered connectivity in which as described in [28] one approach for instance decides to sustain two-degree connectivity even under link or node failure based on moving a subset of the nodes. Although the thought of the nodes movement is comparable to the one of ours, stressing the need for 2-connectivity might restrain the application-level functionality and again may not be practical in large-scale networks of resource-constrained nodes. In this research, the most related method to RIM found in the literature is DARA [29] requiring each of nodes to maintain a list of their 2-hop neighbors and picks a neighbor of the failed node to relocate based on the number of communication links.

Younis et al. [30] in turn have proposed RIM (Recovery through Inward Motion) and NN (Nearest Neighbor) algorithms. RIM, a distributed algorithm for recovery through inward motion, has a major idea that when a node F fails, its neighbors will move inward to its position leading them to be able to link each other. It is because these neighbors refer to the ones directly affected by the F failure, and when being able to reach each other again, the network connectivity would be restored to its pre-failure status. The procedure to relocate is by recursively handling any disconnected node for the movement of one of their neighbors, for instance those having already moved towards the faulty node. Equal to RIM, NN (nearest Neighbor) algorithm pursues voracious heuristics. When a failure occurs in a node, NN for repairing the severed connectivity around F will move to its closest neighbor, which is FNN, to where F is positioned. The neighbors of FNN respond its departure in that the closest one among them will move and settle where FNN used to be, and so on. NN will stop when it is found no neighbor for a departed node (reaching the network periphery) or when all nodes in the network have already moved. Different from RIM applying 1-hop neighbor list, the NN algorithm on the other hand need that every node is aware of its 2-hop neighbors. For this, the nearest neighbor will be recognized before the failure of F. At this point, both RIM and NN are not concerning about the implication of restoring the connectivity on the network coverage. This permanent repositioning avoids by Coverage Conscious Connectivity Restoration (C^3R) algorithm [22]. Through replacing the neighbor node with another node will bring the connectivity back, it in fact merely modify the coverage hole to another part of the field, either in the inner part of the network or at the periphery. It could be coped with by temporarily replacing the failed node with one or multiple of its neighbors only.

3 Problem Statement

The loss of a node due to failure may not only affect the network coverage but also impact network connectivity. The recovery process of proposed technique is initially the same as C3R, clearly shown in Fig. 2. This paper focuses on maintaining network connectivity when a simultaneously node fails, while sustaining the per-failure coverage. The network topology as illustrated in Fig. 2a could be considered as the following samples. The failure of one node or two node would disengage their neighbors from the rest of the network and then will put a hole down in coverage for no other node having its sensing range overlapping with failure node as shown in Fig. 2b. Though replacing failure nodes with another nodes will bring the connectivity back, it in fact merely modify the coverage hole to another part of the field, either in the inner part of the network or at the periphery. It could be coped with by temporarily replacing the failed node with one or multiple of its neighbors. But the actual problem arises when simultaneously node failure occurs. In other words when the participating nodes neighbor failure occur and then the node will decide according to some criteria whether it join which neighbor node. The participated nodes will exchange back and forth leading the network topology and the coverage mostly equal to their pre-failure status. In this paper we proposed simultaneous node failure technique.



(a) Connected mobile nodes network

(b) After nodes failure

Fig. 2. The recovery process

4 Methodology

4.1 Proposed Approach

At first, the occurrence of a redundant node in the network comes to be an efficient solution for coverage and connectivity in that it could substitute the failed node with the spare node.

A. Before Failure Process

In this research, our approach is designed to ask each node to encompass list of 1-hop neighbors that is the only pre-failure knowledge requirement by each node broadcasting a HELLO message to introduce itself to its neighbors nodes sporadically will send the HEARTBEAT messages to their neighbors. At this point, failure node F is assumed to be failed if its neighbor node, node A does not receive a pre-set count of HEARTBEAT messages from a neighboring node that is F. The movement of a node also confirms the neighbors for an error in interpretation and a list of neighbors updated each time one of them changes its position.

B. Synchronization of Neighbors

When the failure of node F is detected by node A while the neighbor nodes (called as concerned nodes) may be in process for all nodes that have 1-hop list, it is then not possible to figure out the neighbor nodes. Nevertheless for the shorter distance from F, node J any of the neighbors node is assumed to reach at first and will act as a recovery coordinator communicating and synchronizing with the rest of them.

C. Recovery Implementation Plan

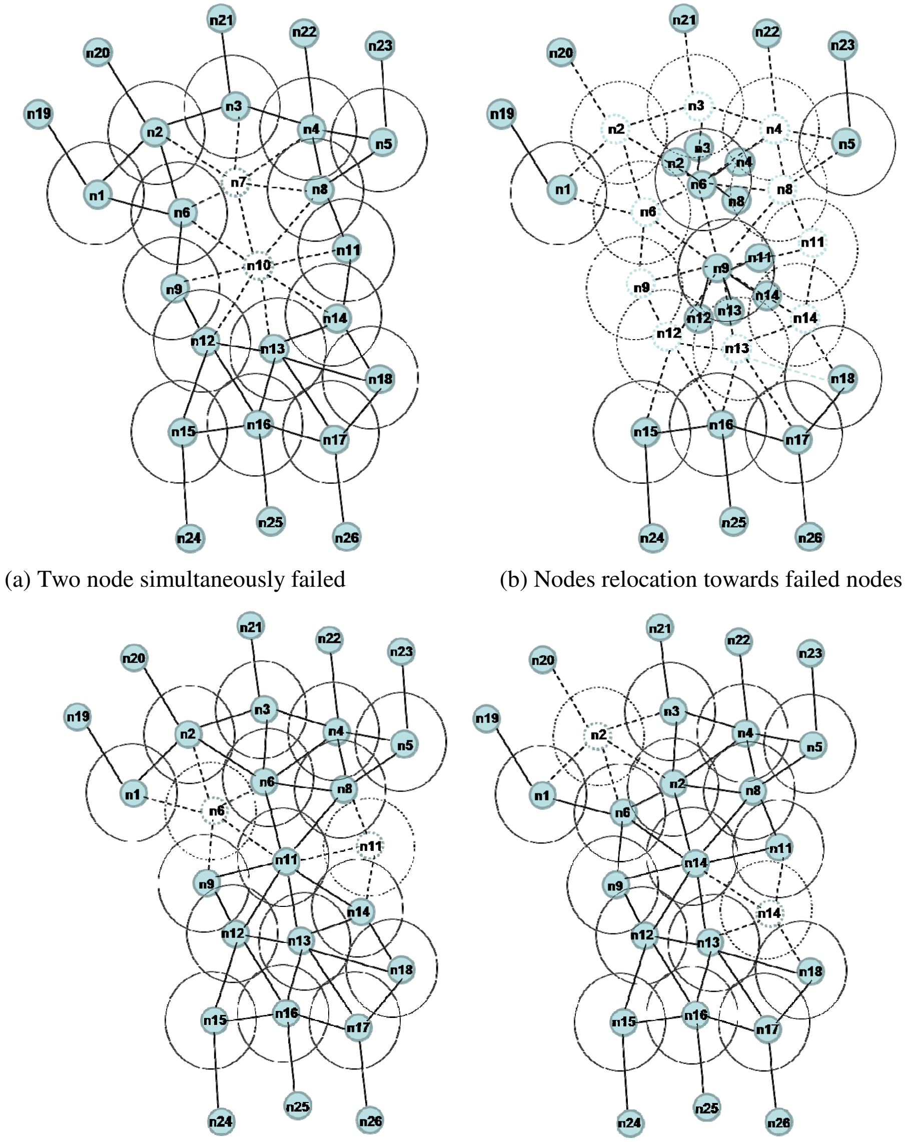
The general key points for crafting and executing the recovery plan are presented as follows:

- It is possible to concerned node A to compute its overlapped coverage, distance to F and energy reserve before moving towards F.
- Each node A confirms to neighbors for temporary relocation in avoiding to declare faulty that neighbor find other route or buffer the data until the return of node A.
- The node close to F will be considered as recovery coordinator if two nodes claim for that. The lowest ID node then will be recovery coordinator for F and broadcast to concerned nodes.
- Recovery coordinator retains the list of ranking determined by the overlap coverage, distance covered, and energy reserve. It then set the priority in round robin fashion.
- When returning, A notifies its neighbors and resumes routing of the buffered data packets. This node after that will repeat an equal prescribed process.
- The node will send the request once going below the threshold. The request will be received by node presently in the position of F. It will be new recovery coordinator and create a new schedule.

The key points for crafting and executing the recovery plan if simultaneous node failure occurs at different time span are presented as follows:

- As shown in the Fig. 3a node 7 and node 9 simultaneously failed and in order to start recovery process the neighbor of the failed nodes will start the recovery process they move towards the failed nodes.
- Node 6 and node 8 both are in the range of failed nodes n7 and n10. Node 6 and node 8 first calculate its overlap coverage and distance with the failed nodes, as shown in the Fig. 3b, Due to high overlapping with the failed node n7, the node n6 and n8 will move towards the n7 to participate in the recovery process.

- According to Fig. 3c Node 6 and node 11 is the first node in the recovery schedule they will relocate to the failed nodes.
- Fig. 3d shows that after relocation back to the initial position of node 6 and node 11. Node 2 and node 14 will relocate to the failed nodes.
- After relocating back to its initial positions according to recovery schedule rest of the nodes will relocate in round robin fashion.



(a) Two node simultaneously failed

(b) Nodes relocation towards failed nodes

(c) First node starts the recovery process

(d) After recovery schedule nodes relocation

Fig. 3. Recovery process for simultaneously nodes failure

4.2 Sensor's Energy Model

We used the model of Rabinar Heinzelman et al. (2000), and Bhardwaj et al. (2001). Communication energy dissipation: In this form, the core energy parameters for communication are the energy/bit absorbed by the transmitter electronics (β11), energy diffused in the transmit op-amp (β2), and energy/bit absorbed by the receiver electronics (β12). By considering a 1/dn path loss, the absorbed energy then comes to be

$$E_{tx} = \langle \beta_{11} + \beta_2 d^n \rangle \times s \tag{1}$$

$$E_{rx} = \beta_{12} \times s \tag{2}$$

Where Etx refers to the energy to send s bits and Erx refers to the energy consumed to receive s bits. Table 1 specifies the energy parameters. From the simulation, it is found that β3 refers to 25 nJ/bit and a sample refers to 10 Kbit which is generated at a steady rate of one per 1000 s. Motion related energy: It is then assumed that a light weight 0.65lb mobile sensor can travel at a steady speed of 2.5cm/s.

Table 1. Parameters for the commutation energy model

Term	Meaning
β_{11} β_{12}	Energy dissipated in transmitter and receiver electronics per bit (take to be 25 nj/bit).
β_2	Energy dissipated in transmitter amplifier (take to be 50 pJ/bit/m^2).
s	Number of bits in the message.
d	Distance that the message traverses.

5 Simulation Results

The simulation experiments involve randomly generated WSN topologies with varying number of nodes and communication ranges. The number of nodes has been set to 25, 50, 75, 100 and 125 in a field with dimensions of 1000×1000 m2. Since RIM and NN don't accommodate different sensing and communication ranges, the values of rs and rc have been kept equal for all experiments that involve these approaches. However for proposed algorithm, experiments were conducted by varying the communication and sensing ranges and the changes in field coverage are measured. The sensing and communication ranges have been set to 25, 50, 75, 100, 125, and 150m. Every node has an initial energy of 100J. The energy consumed in sensing, communication and motion is calculated based on the specified model.

Fig. 4 shows the total distance that nodes collectively had to travel during the recovery as a function of the communication range. Again, the sensing and communication ranges are equals in these sets of experiments. The distance a node would travel depends on the inter-node proximity, which is at most the communication range rc. Therefore, as rc increases, the total distance travelled by a node increases. This is obvious for RIM and NN, where the travelled distance grows at a high rate. Unlike RIM and NN, proposed algorithm limits the node involvement into recovery to only the neighbors of the failed node and avoids the cascaded relocation of RIM and NN. It is worth noting that the proposed algorithm handles well the increase in network connectivity, when rc is large.

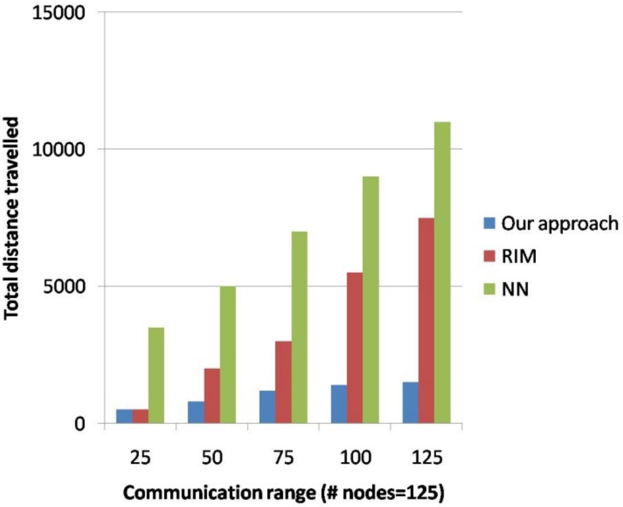


Fig. 4. Total distance travelled by all nodes (meters) vs. communication range (meters) for a network of 150 nodes (The sensing and communication ranges are equal)

6 Conclusion

Maintaining a connected inter-node topology is very crucial in applications of mobile sensor networks. A failure of a node can cause the network to partition and thus disrupt the application. Unlike most prior work that exploits node relocation in order to restore connectivity, proposed algorithm addresses the loss of both connectivity and field coverage. To overcome this problem, proposed algorithm avoids permanent repositioning of nodes. The failure recovery task lies with only neighbors of the failed nodes. These neighbors coordinate among themselves and agree on their role in the recovery. Each node involved in the recovery will move to the position of the failed node to restore connectivity and coverage in that area and then go back to its original position after serving for some time. Initially the algorithm is validated using the performance parameter, distance moved and it is worth noting that our algorithm handles well the increase in network connectivity. These results will help to find the total energy consumption and number of exchanged messages by the mobile node.

References

1. Pompili, D., Melodia, T., Akyildiz, I.F.: Deployment analysis in underwater acoustic wireless sensor networks. In: Proceedings of the ACM International Workshop on Under-Water Networks (WUWNet), Los Angeles, CA (September 2006)
2. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless sensor networks: a survey. Computer Networks 38(4), 393–422 (2002)
3. Sohrabi, K., Gao, J., Ailawadhi, V., Pottoe, G.J.: ULCA, Protocols for self-organization of a wireless sensor network. IEEE Personal Communications 7(5), 16–27 (2000)
4. Min, R., Bhardwaj, M., Cho, S., Sinha, A., Wang, A., Chandrakasan, A.P.: Low power wireless sensor networks. In: Proceedings of International Conference on VLSI Design, Bangalore, India (January 2001)
5. Katz, R.H., Kahn, J.M., Pister, K.S.J.: Mobile networking for smart dust. In: Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 1999), Seattle, WA (August 1999)
6. Jun, H., Zhao, W., Ammar, M.H., Zeguar, E.W., Lee, C.: Trading latency for energy in densely deployed wireless ad hoc networks using message ferrying. Journal of Ad Hoc Networks 5(4), 444–461 (2007)
7. Chu, M., Haussecker, H., Zhao, F.: Scalable information driven sensor querying and routing for ad hoc heterogeneous sensor networks. The International Journal of High Performance Computing Applications 16(3), 293–313 (2002)
8. Dasquapta, K., Kalpakis, K., Namjoshi, P.: An efficient clustering-based heuristic for data gathering and aggregation in sensor networks. In: Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC 2003), New Orleans, LA (March 2003)
9. Lindsey, S., Raghavendra, C.S., Sivalingam, K.: Data gathering in sensor networks using the energy*delay metric. In: Proceedings of the IPDPS Workshop on Issues in Wireless Networks and Mobile Computing, San Francisco, CA (April 2001)
10. Younis, M., Munshi, P., Al-Shaer, E.: Architecture for efficient monitoring and management of sensor networks. In: Proceedings of the IFIP/IEEE Workshop on End-to-End Monitoring Techniques and Services (E2EMON 2003), Belfast, Northern Ireland (September 2003)
11. Heinzelman, W., Chandrakasan, A., Balakrishnan, W.: An Application-Specific Protocol Architecture for Wireless Microsensor Networks. IEEE Transactions on wireless Communicarions 1 (October 2002)
12. Clouqueur, T., Phipatanasuphorn, V., Ramanathan, P., Saluja, K. K.: Sensor Deployment Strategy for Target Detection. In: First ACM International Workshop on Wireless Sensor Networks arid Applications (2002)
13. Pottiz, G.J., Kaiser, W.J.: Wireless Integrated Network Sensors. Communications of the ACM (May 2000)
14. Akkaya, K., Younis, M.: COLA: A Coverage and Latency aware Actor Placement for Wireless Sensor and Actor Networks. In: The Proceedings of IEEE Vehicular Technology Conference (VTC-Fall 2006), Montreal, Canada (September 2006)

15. Melodia, T., Pompili, D., Gungor, V.C., Ikyildiz, I. F.: A Distributed Coordination Framework for Wireless Sensor and Actor Networks. In: The Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (Mobihoc 2005), Urbana-Champaign, Illinois (May 2005)
16. Basu, P., Redi, J.: Movement Control Algorithms for Realization of Fault-Tolerant Ad Hoc Robot Networks. IEEE Networks 18(4), 36–44 (2004)
17. Akkaya, K., Younis, M., Bangad, M.: Sink Repositioning for Enhanced Performance in Wireless Sensor Networks. Elsevier Computer Networks 49, 512–534 (2005)
18. Liu, X., Xiao, L., Kreling, A., Liu, Y.: Optimizing Overlay Topology by Reducing Cut Vertices. In: The Proceedings of ACM International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV 2006), Newport, Rhode Island (May 2006)
19. Dhillon, S.S., Chakrabarty, K.: Sensor placement for effective coverage and surveillance in distributed sensor networks. In: Proc. IEEE Wireless Commun. Netw. Conf., pp. 1609–1614 (2003)
20. Biagioni, E., Sasaki, G.: Wireless sensor placement for reliable and efficient data collection. In: Proc. Hawaii Int. Conf. Syst. Sci., p. 127b (2003)
21. Howard, A., Mataric, M.J., Sukhatme, G.S.: Mobile sensor network deployment using potential fields: A distributed scalable solution to the area coverage problem. In: Proc. 6th Int. Conf. Distributed Autonomous Robotic Syst., Fukuoka, Japan, pp. 299–308 (2002)
22. Tamboli, N., Younis, M.: Coverage-aware connectivity restoration in mobile sensor networks. Journal of Network and Computer Applications 33(3), 363–374 (2010)
23. Younis, M., Akkaya, K.: Strategies and techniques for node placement in wireless sensor networks: A survey. The Journal of Ad-Hoc Networks 6(4), 621–655 (2008)
24. Wang, G., Cao, G., La Porta, T.: Movement-assisted sensor deployment. In: Proceedings of the 23rd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2004), Hong Kong (March 2004)
25. Heo, N., Varshney, P.K.: Energy-Efficient Deployment of Intelligent Mobile Sensor Networks. IEEE Trans. on Systems, Man, Cybernetics, Part A 35(1), 117–127 (2005)
26. Wang, G., Cao, G., La Porta, T.: Proxy-based sensor deployment for mobile sensor networks. In: Proceedings of the 1st IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS 2004), Fort Lauderdale, Florida (October 2004)
27. Wang, G., Cao, G., La Porta, T., Zhang, W.: Sensor Relocation in Mobile Sensor Networks. In: The Proceedings of the 24th Annual IEEE Conf. on Computer Communications (INFOCOM 2005), Miami, FL (March 2008)
28. Abbasi, A., Baraudi, U., Younis, M., Akkaya, K.: C2AM: An Algorithm for Application-Aware Movement-Assisted Recovery in Wireless Sensor and Actor Networks. In: The Proceedings of the IEEE International Conference on Wireless Communications and Mobile Computing, Leipzig, Germany (June 2009)
29. Abbasi, A., Akkaya, K., Younis, M.: A Distributed Connectivity Restoration Algorithm in Wireless Sensor and Actor Networks. In: The Proceedings of the 32nd IEEE Conf. on Local Computer Networks (LCN 2007), Dublin, Ireland (October 2009)
30. Younis, M., Lee, S., Gupta, S., Fisher, K.: A localized self-healing algorithm for networks of moveable sensor nodes. In: Proceedings of the IEEE Global Telecommunications Conference (Globecom 2008), New Orleans, LA (November 2008)

A Survey on Topology Maintenance Techniques to Extend the Lifetime of Wireless Sensor Networks

Amna Shahid and Hassaan Khaliq Qureshi

School of Electrical Engineering & Computer Science (SEECS)
National University of Sciences & Technology (NUST), Pakistan
{amna.shahid,hassaan.khaliq}@seecs.edu.pk

Abstract. Wireless Sensor Network (WSN) is a well known technology due to its applications in diverse fields including both civil and military domain. However, being battery powered, the network lifetime of WSN is hugely dependent on how efficiently this battery power is utilized. Topology Control consisting of Topology Construction and Topology Maintenance, is a popular technique to conserve energy and extend the lifetime of WSN by building and maintaining a reduced topology that offers both connectivity and coverage. Topology Maintenance rebuilds a new topology once the current topology is no longer optimal. In this survey, our focus is on the issue of energy efficiency and we have presented a thorough analysis of current topology maintenance techniques for prolonging the battery lifetime of wireless sensor nodes. We have classified Topology Maintenance according to the energy conservation technique adopted by each algorithm, and have evaluated them on the basis of trade-offs offered by each approach to guide designers in opting for a technique that fulfills their application needs. In addition, we also provide insight with the help of simulation results.

Keywords: Topology Maintenance, WSN lifetime , Energy conservation.

1 Introduction

Recent advancements in technology have made it possible to deploy small, low-power, low-cost, and distributed devices, that are able to perform self-processing, self configuration and having capability of wireless communication [1]. These devices are known as motes or sensor nodes and the network formed by these devices is known as a Wireless Sensor Network (WSN). Because of the limitation in size and cost, each node in the WSNs can support only restricted processing, however, when coordinated with the data received from countless other nodes present in the network they have the capability to measure and report a given physical environment in elaborate detail [2].

The significant challenges for the realization of WSNs are its resource restraints. Being minute in size and inexpensive WSNs are susceptible to failure. The most fundamental issue in the functioning of WSNs is that wireless sensor

F.K. Shaikh et al. (Eds.): WSN4DC 2013, CCIS 366, pp. 96–107, 2013.

nodes have a very constrained allocation of energy [3]. Most of the sensor nodes are battery powered and battery is not an infinite source of energy, therefore the energy of battery powered sensor nodes depletes after a period of time. It is not practical to change these batteries frequently particularly in harsh or unreachable environments and conditions. Therefore, the only viable option left is to use whatever available energy there is wisely, so that the nodes battery lifetime can be extended. The lifetime of the WSNs greatly depends upon individual nodes energies. Therefore, energy efficiency is the most critical issue in WSNs. In order for nodes to have an extended period of autonomy, algorithms/protocols that enable in optimizing battery usage are required, so that the life of individual nodes and the lifespan of the network as a whole can be extended [4].

To guarantee network longevity, reliability, security and survivability, WSNs are required to have strong network recovery capabilities. Therefore, the requirement of network maintenance algorithms/protocols becomes more and more important [5].

Topology Maintenance (TM) is a critical issue in WSNs. Once the initial topology built by Topology Construction (TC), is no longer optimal, Topology Maintenance is invoked which recreates the existing topology, thus extending the lifetime of network. Many TM algorithms/protocols exist in literature. The choice of topology maintenance algorithm plays an important role in the lifetime and functioning of network.

In this survey paper, we have examined and analysed various topology maintenance techniques existing in literature. We have covered recent developments in this area including prior work done in this area. What differentiates our survey from earlier works is manner in which topology maintenance techniques are classified. We have characterized TM schemes into two classes, distributed and centralized.

The rest of the paper is divided as follows. Section II provides an overview of Topology Control. Section III gives a description of the main types of Topology Maintenance techniques and gives a brief overview of the latest and most popular topology maintenance techniques existing in literature. Section IV presents the performance evaluation. Finally, the paper is concluded in Section V.

2 Related Work

Topology Control is an efficient way of conserving energy of battery powered sensor nodes. Topology control is comprised of two components namely; topology construction and topology maintenance.

Topology construction is the initial process of building a reduced topology once the sensor nodes are deployed and activated [6].Topology construction mechanisms ensure that the new topology built will result in better energy conservation at the same time making sure that the network remains connected and provides maximum coverage.

While TC is invoked only once at the start, TM is a continuous process that starts after the initial topology has been constructed. TM is described as the process that recreates or rotates the topology of the network, whenever the current topology is no more sufficient.

The topology maintenance protocols leverage node redundancy. These algorithms maintain the topology of the network and the state of the nodes, rotating the role of nodes between an active and sleep state. The main idea behind the application of these techniques is to keep as few active nodes as attainable [7]. The active nodes selected by these protocols should be adequate to provide network connectivity and/or the sensing coverage. This scheduling of nodes, keeping only those nodes active that will keep the network connected and covered, results in extending the network lifetime.

The main focus of this survey is on topology maintenance schemes that extends network lifetime by maintaining active and inactive nodes.

2.1 Design Issues in Topology Maintenance

For an efficient topology maintenance process that provides the anticipated outcome in terms of prolonging the network lifetime, it is important that the TM techniques must be designed such that they fulfill the following conditions:

Energy efficiency: The topology maintenance technique must be energy efficient and the topology maintenance process should result in reducing the energy consumption.

Low overhead: Number of messages exchanged should be controlled as it creates an overhead and ultimately results in extensive consumption of energy.

Low convergence time: When a new topology takes over the old one, there is a transition time during which the takeover takes place and during this time the network or part of the network remains inactive. Therefore, it is important to keep this transition time/convergence time as low as possible.

Memory consumption: As sensor nodes have limited memory, it is important to design our algorithms that take into account this aspect.TM techniques such as static global (described later) that pre-calculate and store all the possible topologies beforehand use up a lot of memory.

2.2 Classification of Topology Maintenance Algorithms

Topology maintenance can be classified into several categories based on when TM process takes place, the triggering criteria and their scope.

Time of Building Reduced Topology. Based on time of creating the new topology, TM techniques are classified as Static, Dynamic and Hybrid TM techniques.

The protocols based on Static TM rotate existing topology with any one of the pre calculated topologies when needed. Static TM algorithms pre-calculate all possible topologies at the time of topology construction and store these topologies in memory. Although static techniques take an additional time during TC as they have to calculate several possible topologies, but they take least amount of time during TM process. A drawback with static techniques is that these protocols do not take into account the current status of the network.

Dynamic Topology Maintenance algorithms as the name implies are dynamic creating topologies on the fly. Although dynamic TM techniques take longer during recreating topologies and take extra resources every time they are run, but the obvious advantage is that dynamic techniques use the current network information while recreating topologies.

Hybrid Topology Maintenance technique is a combination of both static and dynamic techniques. In Hybrid TM, several topologies are calculated during the TC process as in static techniques. However, when the static topologies can no longer be applied the mechanism finds a new topology dynamically.

Triggering Criteria. Another important criteria when designing and selecting a TM protocol is the triggering criteria, that is what triggers the TM process. Triggering criteria plays an important role in the functioning of WSNs in terms of their energy consumption, coverage and/or reliability. Most of the TM protocols are either time- based, energy based or in some cases failure or density based.

Scope of the network. Scope of TM may either be global or local. Global or Centralized TM algorithms involve all the network nodes during TM for making a global optimal decision. In most cases, the global technique involves the sink node, which makes topology recreation decision and all the other nodes change their topology accordingly. In most of the cases, global TM switches the complete network topology.

On the contrary, a local or distributed TM technique involves only a small subset of nodes while making a local optimal decision. The advantage that this technique offers is that as it involves only a limited subset of nodes, this technique results in consuming less energy as compared to a global technique.

In this survey paper, we have focused on distinguishing the existing centralized topology maintenance schemes from distributed schemes. In the next section, a detailed analysis of both of these schemes is given including their inherent benefits and drawbacks.

3 Centralized vs. Distributed Topology Maintenance Schemes

As discussed in Section II, in centralized TM solutions, the sink node makes the recreation decision. The new topology is then broadcast to the entire network. Although centralized or global approaches are applicable in most of the scenarios and are easier to develop, these approaches have a single point of failure and may result in increased overhead particularly when the network size is increased and information has to transverse through several hops. Distributed TM schemes work on a small scale of nodes particularly those nodes that are in the neighbors of the node that has to be replaced. Some prominent global and local TM schemes are discussed below.

3.1 Distributed Topology Maintenance Schemes

Distributed or local topology maintenance schemes involve a limited number of nodes. Recent research has been focused on developing distributed Topology Maintenance techniques as these techniques can guarantee efficient energy consumption. Some of the latest and most popular TM techniques in this area are discussed below.

DL-DSR. Dynamic Local DSR or DL-DSR is a distributed energy based distributed and dynamic TM technique which follows the Dynamic Source Routing (DSR) [8] protocol for wireless networks. DL-DSR follows CDS based approach where nodes are arranged hierarchically in a parent child manner. It is a dynamic protocol which is initiated whenever the energy of a node drops below a threshold.

The protocol works in two phases to find substitute for a node whose energy has depleted to a specific level. The substitute node must be able to take over the new orphaned child nodes. The protocol explained in [9] sends Wakeup and Route Request messages to the neighboring nodes to replace the parent node whose energy has depleted with a new parent node which takes over all orphaned nodes.

The topology is recreated locally, without the need of involving the sink node. The benefit of this protocol is that it has small message overhead as compared to global techniques. The main advantage is that with the increase in the node density, the message overhead remains almost constant.

Efficient Topology Maintenance Scheme for Wireless Sensor Networks. Efficient Topology Maintenance Scheme for Wireless Sensor Networks or EETMS [10] is also a distributed and dynamic TM protocol. This protocol is failure based.

EETMS recreates topologies by controlling the transmission power of the neighboring nodes of the failed node, such that the network remains connected. There are two strategies proposed in [10] that achieves this goal. The first strategy is to connect all immediate neighbors of faulty node by adjusting the transmission power of all immediate nodes. This approach connects all immediate nodes of faulty node with the shortest link.

In the second strategy, the approach is to achieve a connected local network with the minimal possible power (the sum of the path lengths) using a Breadth First Search (BFS) mechanism.

Authors in [10] have shown that EETMS results in lesser power stretch factor which indicates lower energy consumption as compared to similar protocols that work on the same principle such as RLS [13] and other new power based Topology Maintenance scheme proposed in [11], [12]. The authors have also shown that over time EETMS gives more number of active neighbors as compared to RLS thus indicating an increase in lifetime of the network. The drawback of this approach is that, although it conserves the network energy in an efficient manner but it is a failure based approach that means that a nodes energy is completely drained out before it starts the maintenance process. This means high convergence time as there may be several dead nodes in the network.

ASCENT. Adaptive Self-Configuring Sensor Network Topology or ASCENT [7] is a distributed protocol capable of self-reconfiguration. This protocol allows nodes to monitor operating conditions locally. On the basis of these conditions, nodes make a decision whether or not they should be participating in routing. For achieving efficiency of energy, ASCENT picks only a subset of nodes to stay in an active state that act as routing backbone. Rest of the nodes in the network remain in a passive state. The nodes that are passive periodically listen to other neighboring nodes for inspecting whether they have to become part of the routing backbone by changing to active state. For instance, when there is a higher rate of packet loss, the passive nodes are turned active in order to preserve connectivity. Otherwise the passive nodes keep their radios turned off to save battery power.

Nodes in ASCENT remain in one of the four states, namely test state, passive state, active state and sleep state [7].

The advantage of this protocol is that it is self-reconfigurable and adaptive to react to applications dynamic events. However, its disadvantage is that due to uneven load distribution it may result in rapid energy depletion among active nodes.

It is worth mentioning that ASCENT takes topology control as a single process and does not separates the maintenance part. Therefore, it cannot be used with many TC algorithms such as A3 [14], EECDS [15], A1 [16]. For the maintenance part of such algorithms, we require a topology maintenance algorithm that should be integrated with topology construction algorithms. To the best of our knowledge, such algorithms are very rare and each algorithm is designed to fill its own gap. As an example, EEMTS only takes failure as the criterion to switch the topology. However, in many critical applications, we want to trigger the topology based on the energy threshold. Similarly, distributed CDS based topology construction algorithms have been proposed (A3, EECDS, A1), but their topology maintenance part is completely centralized. Table 1 distinguishes the three distributed topology maintenance algorithms based on their design principles.

3.2 Centralized Topology Maintenance Schemes

Centralized TM schemes such as Dynamic Global Energy based Topology Recreation (DGETRec) and Dynamic Global Time based Topology Recreation (DGTTRec) are very prominent TM algorithms/protocols due to their simplicity and practicality. Although the focus of recent research has shifted to distributed techniques, but global techniques continue to be employed in WSNs. Centralized TM protocols are divided on the basis of when the topologies are built. The three main types of centralized topology maintenance schemes are discussed below.

Static Global Topology Rotation (SGTRot). The Static Global Topology Rotation is a centralized and static approach for rebuilding topologies. It can

Table 1. Comparison of Distributed Topology Maintenance Algorithms

Design issues	**DL-DSR**	**ASCENT**	**EETMS**
TM Mode	CDS based	CDS based	Power control
TC/TM	TM	both TC and TM	TM
Triggering criteria	Energy based	Energy based	Failure based
Energy Efficiency	High	Medium	High
Message overhead	Low	Medium	Low
Integration with TC algorithms	All CDS TC algos	TC algo same as TM algo	not applicable on CDS based TC algos

either be time triggered or energy triggered. SGTRot builds multiple reduced topologies during TC phase and these topologies are rotated when the current topology needs to be changed. The main assumption of Static Global techniques is that nodes keep track of several Virtual Network Interfaces, or VNIs at a time. These VNIs include information pertinent to a node regarding each individual reduced topology created in the network like: address, state of the node (active, inactive or sink), routing information, etc. Whenever a topology has to be rotated, each node quickly converges to a new VNI.

The protocol is quite simple. Whenever a trigger is initiated in any of the nodes, it will transmit a Notification Message to the sink node thus intimidating the sink node that its trigger has gone off. On receiving the Notification message, the sink node decides whether the occurrence of the triggering event is sufficient enough to initiate the rotation process. If the sink node decides that it does not have sufficient active nodes in the neighborhood it will rotate the topology by moving on to the next VNI. After each rotation, the sink node evaluates whether there is at least one active neighboring node. If there are no active nodes in the sinks neighborhood, the network is considered dead.

Dynamic Global Topology Recreation. The Dynamic Global Topology Recreation (DGTRec) is perhaps the most frequently employed topology maintenance techniques as it is the simplest technique and does not require any pre calculated information or VNI and can be easily employed over any type of sensor network. Another reason for their popularity is because these protocols are closely associated with the topology construction protocols.

Based on the triggering criterion, DGETRec is further classified into two types namely Dynamic Global Energy-based Topology Recreation (DGETRec) and Dynamic Global Time-based Topology Reconstruction (DGTTRec). DGETRec is an energy based scheme, thus a topology is recreated once the energy of a node drops below a threshold while DGTTRec is a time based approach which is initiated after particular time intervals.

Similar to SGTRot, topology maintenance is initiated whenever the triggering criterion is met. The bottleneck node will send a Notification Message to the sink node, notifying the sink node that an event has occurred. On the arrival of the Notification message to the sink node, the sink node makes a decision whether or not the occurrence of this triggering event is reason enough to initiate the topology rotation process. In the scenario, in which sink node considers that a rotation is crucial for the network, the sink node will transmit a Reset Message and, if it is the only sink in the topology, it will schedule a new execution of the topology construction protocol initially applied to reduce the topology. On receiving a Reset Message, a node will immediately forward that message to all its neighboring nodes and then the node will get rid of all the information related to the current reduced topology, and will move itself into the initial state of the topology construction protocol, where it waits for new execution [17].

Hybrid Global Topology Recreation and Rotation. HGTRecRot or Hybrid Global Topology Recreation and Rotation combines the best of both static and dynamic techniques giving us a protocol that works both statically and dynamically. Like a static protocol, HGTRecRot creates several VNIs at the start of TC and when needed these VNIs can be applied as in the case of static protocols. However, once the calculated VNIs cannot be applied for example when the sink node detects it has been isolated from the network, HGTRecRot invoke dynamic topology maintenance. The sink node then transmits a Reset message to all its neighbors which is forwarded to rest of the network. By sending a Reset message the sink node invokes the TC to update the current VNI as in DGTRec. After resetting the current VNI, the sink node still remains isolated, it will eliminate the current VNI from the list of available ones and will rotate to the next VNI. If there are no more VNIs available, then the sink will determine that the network is dead [17].

4 Performance Evaluation

In order to evaluate the algorithms, in this section, we summarize our findings by performing simulations to study the performance of some topology maintenance algorithms. All simulations are done in Atarraya [18], an event driven simulator that caters for topology construction, maintenance and sensor and coverage protocols. The purpose of these simulations is to determine which TM algorithm will result in efficient energy consumption. Topology Maintenance algorithms have been applied over A3 Topology Construction algorithm [14] in both sparse and dense networks.

Although this survey paper has included TM techniques based on power control but our survey only includes CDS based TM approaches as power based approaches come under another class of power management techniques. In addition to this power based and location based approaches are expensive and difficult to implement.

The following assumptions are made in all the evaluations.

- Nodes are placed in a 2-Dimensional space.
- Nodes do not have any information about their or their neighbors location, position or orientation.
- All nodes are incapable of motion.

We have conducted analysis on number of messages exchanged during each of the TM protocol and the spent energy ratio. These two metrics can provide us with an insight into how each of the TM protocol utilizes energy, which in turn will determine the network lifetime. Table 2 shows a summary of important simulation parameters that were considered during simulation. All values have been averaged over 100 simulations each.

Table 2. Simulation Parameters

Deployment Area	300m x 300m
Number of sink nodes	1
Number of nodes	50-250
Node Location Distribution	Uniform
Node Energy Model	Mote
Communication Radius	100m
TM Energy Threshold Step	0.9

4.1 Number of Messages Sent

Communication is the most energy consuming tasks among all of the operations of WSNs. While designing topology maintenance and construction protocols reducing the number of messages exchanged is at the top priority of protocol designers.

Our analysis shows that centralized or global techniques where topology recreation messages are exchanged with the sink node result in greater message overhead. On the other hand distributed topology maintenance techniques like Local DSR results in fewer number of exchange of messages as shown in Figure 1.The trend in Figure 1 shows that as the number of nodes in the network is increased, the number of messages exchanged in centralized approaches particularly in DGETRec increases exponentially while it remains somewhat constant in distributed approaches like local DSR. Although stationery global techniques also exchange fewer number of messages but as mentioned earlier, these approaches cannot predict the status of the network and may therefore result in topologies that result in inefficient energy consumption.

As the node density is increased, in global protocols such as DGETRec, the rate of increase of number of messages goes up while in distributed protocols such as Local DSR, this rate remains somewhat constant.The reason is that in

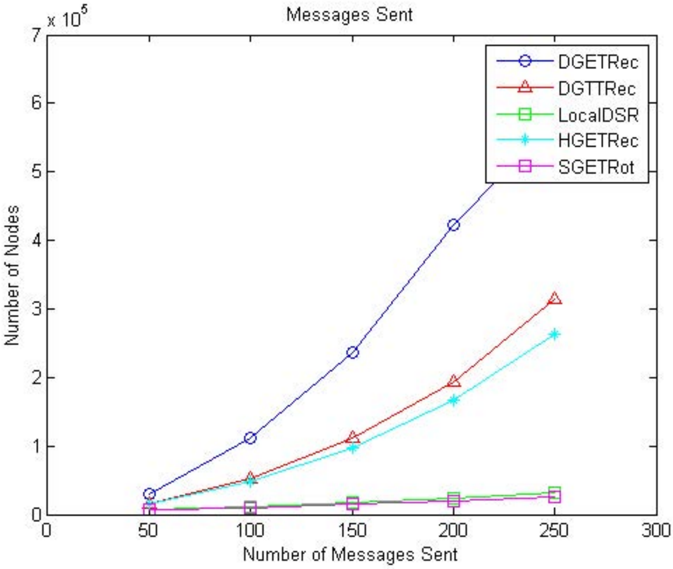


Fig. 1. The total number of messages exchanged vs. number of nodes

centralized approaches, as node density is increased, notification messages to sink and then reply message will have to transverse several hops. This means that the message overhead is increasing as the number of nodes are increased. While, in the case of distributed schemes, the message flooding is limited to a specific region, so even if number of nodes in the network increases, messages will be exchanged within a limited subset of nodes.

On the other hand, static schemes are shown to have less number of message overhead. Although static schemes may give a lower message overhead as they require fewer messages to switch to a new one, but static techniques do not guarantee an improved network lifetime.

4.2 Spent Energy Ratio

The graph on spent energy ratio of centralized and distributed TM techniques is shown in Figure 2. The figure shows that DGETRec has the highest spent energy ratio while Local DSR has the lowest. Spent Energy Ratio is consistent with number of messages exchanged. As the number of messages exchanged increases or decreases so does the spent energy ratio. This shows that amount of energy spent in topology maintenance is directly related to the number of messages exchanged. A protocol that guarantees fewer number of messages exchanged will be utilizing less energy during topology maintenance.

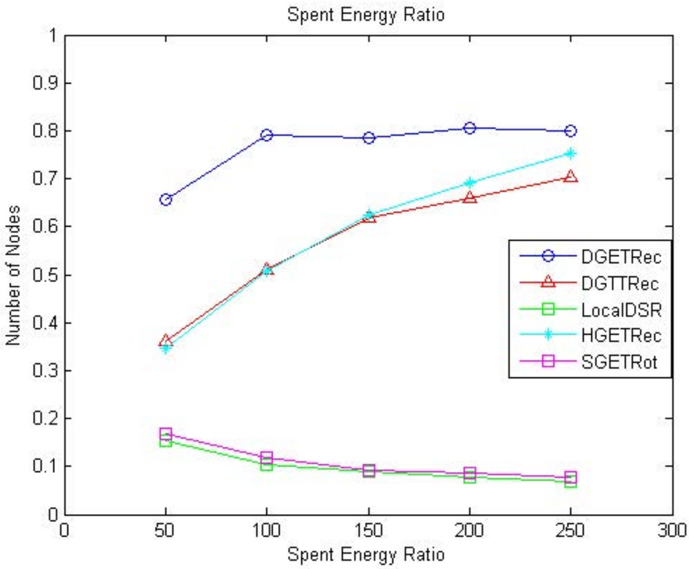


Fig. 2. Spent Energy Ratio vs. number of nodes

5 Conclusion

This papers gives a detailed analysis on Topology Maintenance and the different types of topology maintenance techniques existing in literature. The paper has distinguished centralized topology maintenance schemes from distributed topology maintenance schemes.

In addition to this, the paper includes a performance evaluation of dynamic, static and hybrid centralized and distributed topology maintenance algorithms. We have used number of messages exchanged and spent energy ratio, as a performance metric to determine energy consumption trends in various topology maintenance protocols. Our simulations have shown that local and distributed techniques provide a lower message overhead as compared to global techniques particularly in dense networks. Similarly, distributed solutions currently present are not generic and therefore distributed topology maintenance algorithms are required, which can be used with topology construction algorithms. Therefore, to the best of our believe, the research community working in this domain, would like to see generic distributed topology maintenance algorithms in future.

References

1. Akyildiz, F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless Sensor Networks: A survey. Computer Networks 38, 393–422 (2002)
2. Bharathidasan, A., Ponduru, V.A.: Sensor Networks: An Overview, TechReport, vol. 2 (2002)

3. Song, G.L., Wang, M., Ying, X., Yang, R., Zhang, B.Y.: The Application of Wireless Sensor Network in Agriculture Information Collection. Applied Mechanics and Materials 263, 872–877 (2012)
4. Baker, D.J., Ephremides, A.: The architectural organization of a mobile radio network via a distributed algorithm. IEEE Transactions on Communications, COM-29, 1694–1701 (1981)
5. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: A Survey on Sensor Networks. IEEE Communications Magazine 40(8), 102–114 (2002)
6. Pan, J., Hou, Y.T., Cai, L., Shi, Y., Shen, S.X.: Topology Control for Wireless Sensor Networks. In: Proc. of the 9th ACM MobiCom (2003)
7. Cerpa, A., Estrin, D.: Ascent: Adaptive self-conguring sensor networks topologies. IEEE Trans. Mobile Computing 3(3), 272–285 (2004)
8. Johnson, D.B.: Routing in Ad Hoc Networks of Mobile Hosts. In: Proceedings of the Workshop on Mobile Computing Systems and Applications (WMCSA 1994), pp. 158–163. IEEE Computer Society, Santa Cruz (1994)
9. Johnson, D.B., Maltz, D.A., Broch, J.: DSR: The Dynamic Source Routing Protocol for Multi-hop Wireless Ad hoc Networks. In: Perkins, C.E. (ed.) Ad hoc Networking. ch. 5, pp. 139–172. Addison Wesley (2000)
10. Yin, R., et al.: An Energy Efficient Topology Maintenance Scheme for Wireless Sensor Networks. Journal of Information and Computational Science 8(13), 2815–2822 (2011)
11. Chiwewe, T.M., Hancke, G.P.: A Distributed Topology Control Technique for Low Interference and Energy Efciency in Wireless Sensor Networks. Proceedings of IEEE Transactions on Industrial Informatics 8(1), 11–20 (2012)
12. Cardei, M., Du, D.: Improving wireless sensor network lifetime through power-aware organization. ACM Wireless Networks (May 2005)
13. Shen, Z., Chang, Y.L., Zhang, X., et al.: An efficient topology maintenance algorithm based on shortest path tree for wireless sensor networks. In: Parallel and Distributed Computing, Applications and Technologies, PDCAT, Dalian, December 5-8, pp. 288–292 (2005)
14. Wightman, P.M., Labrador, M.A.: A3: a topology control algorithm for wireless sensor networks. In: Proceedings of the IEEE GLOBECOM (2008)
15. Yuanyuan, Z., Jia, X., Yanxiang, H.: Energy efficient distributed connected dominating sets construction in wireless sensor networks. In: Proceeding of the 2006 ACM International Conference on Communications and Mobile Computing, pp. 797–802 (2006)
16. Qureshi, H.K., Rizvi, S., Khayam, S.A., Rakocevic, V., Rajarajan, M.: A1: An Energy Efficient Topology Control Algorithm for Connected Area Coverage in Wireless Sensor Networks. Elsevier Journal of Network and Computer Applications 35, 597–605 (2012)
17. Wightman, P.M., Labrador, M.A.: Topology maintenance: extending the lifetime of wireless sensor networks. In: 2009 IEEE Latin-American Conference on Communications, LATINCOM 2009, Medellin, pp. 1–6 (September 2009)
18. Wightman, P.M., Labrador, M.A.: Atarraya: A Simulation Tool to Teach and Research Topology Control Algorithms for Wireless Sensor Networks. In: Create-Net 2nd International Conference on Simulation Tools and Techniques, SIMUTools (2009)

INDIGO: Secure CoAP for Smartphones
Enabling E2E Secure Communication in the 6IoT

Daniele Trabalza[1], Shahid Raza[1], and Thiemo Voigt[1,2]

[1] Swedish Institute of Computer Science, Stockholm, Sweden
[2] Department of Information Technology, Uppsala University, Sweden
{daniele,shahid,thiemo}@sics.se

Abstract. With the inception of 6LoWPAN, it is possible to connect wireless sensor networks (WSN) and smart objects with the Internet using the IPv6 protocol, hence forming the IPv6-based Internet of Things (6IoT). Since the links in the 6IoT are lossy, UDP rather than TCP is mostly used for the communication between things. For the same reason, CoAP, a connection-less variant of HTTP, is being standardized as the web protocol for the 6IoT. Due to the sensitivity of the potential applications and presence of humans in the loop, End-to-End (E2E) security between constrained devices and hosts on Internet is one of the main requirements in the 6IoT. Secure CoAP (CoAPs) is used to provide end-to-end security in the CoAP-based 6IoT.

Smartphones with sensing capabilities, direct human interaction, Internet connectivity, and relatively powerful processing and storage capabilities, are going to be an integral part of the 6IoT. In this paper we design, implement, and evaluate CoAPs for Android powered smartphones. We call our CoAPs INDIGO. To the best of our knowledge this is the first work that provides CoAPs support in smartphones. We implement and evaluate all cryptographic cipher suites proposed in the CoAP protocol, including the certificate-based authentication using Ecliptic Curve Cryptography (ECC). We also present novel application scenarios that are enabled by INDIGO on smartphones.

1 Introduction

The Internet of Things (IoT) or strictly speaking IPv6-connected IoT (6IoT) is a hybrid network of IPv6 over Low-power Wireless Personal Area Networks (6LoWPANs) [1] or IP-connected WSNs, and the conventional Internet. At one end the devices in the 6IoT are too resource constrained, for example wireless sensors, and on the other end the device can be any Internet connected device such as a smartphone, a PC or a cloud. Smartphones are becoming an integral part of the 6IoT mainly because they are the most convenient and readily available tools that humans can use to connect to the 6IoT in order to interact with smart objects or *things*.

The Constrained Application Protocol (CoAP) [2] is a new web protocol designed to complement the 6IoT with web capabilities. Smart objects in the 6IoT

F.K. Shaikh et al. (Eds.): WSN4DC 2013, CCIS 366, pp. 108–119, 2013.

are resource constrained and form low-power and lossy networks. As the links are lossy it is hard to maintain a reliable connection using the Transmission Control Protocol (TCP). Hence, the User Datagram Protocol (UDP) is mostly used in the 6IoT. The Hypertext Transfer Protocol (HTTP), however, cannot work over UDP and therefore a new web protocol is required. Towards this end, CoAP is being standardized. CoAP works over UDP and is a connection-less protocol where reliability is achieved with acknowledgements. CoAP proposes to use Datagram Transport Layer Security (DTLS) as a security protocol for automatic key management, data confidentiality, and data integrity. Similar to secure HTTP (HTTPS), CoAP with DTLS support is termed as secure CoAP (CoAPs). CoAPs is being standardized to secure the future 6IoT. The 6IoT devices can securely access web resources using CoAPs as: **coaps://myIP:port/res.xml**, similar to **https://myIP:port/res.xml**

In order to securely access these resources and interact with smart objects it is important to have CoAPs capabilities on the Internet connected devices. In this paper we design and implement the CoAPs protocol, that we call INDIGO, for Android smartphones. Having CoAPs capabilities in smartphones enables numerous applications where smartphones can be securely used in the context of the 6IoT; we discuss these applications in Section 4. We also evaluate the overhead of INDIGO's Handshake and Record protocols and the additional processing and communication requirements of CoAPs.

The next section gives an overview of the technologies used in INDIGO. Section 3 describes the capabilities of INDIGO and details its client and server components. We discuss applications enabled by INDIGO in Section 4. In Section 5 we detail INDIGO's implementation for the Android OS. Section 6 presents our performance evaluation of INDIGO. We discuss related work in Section 7 and conclude the paper in Section 8.

2 Background

Here we discuss the technologies involved in the development of INDIGO.

2.1 IPv6-Connected Internet of Things (6IoT)

The IPv6-connected Internet of Things (6IoT) is a heterogeneous network of tiny devices (*things*) that sense the physical world. The things usually form a WSN or 6LoWPAN network [1] that is connected to the Internet through the Internet Protocol version 6 (IPv6). Things in WSNs/6LoWPANs are resource constrained low power devices. Networks of such devices are also called Low-power and Lossy Networks (LLNs). The things in the 6IoT can be any electronic appliance, smartphone, a standard computer, etc. This heterogeneity in the 6IoT makes it much more challenging to securely connect all 6IoT devices unless standardized protocols exist. The Internet Engineering Task Force (IETF) is actively working on the standardization of 6IoT technologies and has already standardized protocols such as CoAP [2], 6LoWPAN [1] [3], RPL [4].

Due to the lossy links among constrained devices in the 6IoT it is hard to maintain a reliable connection using TCP. Therefore UDP is mostly used in LLNs. The connection-oriented web protocol HTTP cannot work over UDP. Therefore a new protocol is needed and hence CoAP has been designed. To enable seamless End-to-End (E2E) communication and security all devices in the 6IoT should understand each others language. In the 6IoT 6LoWPAN Border Routers (6BRs)/sink can be used between 6LoWPANs/WSNs and the Internet to perform protocol conversion between the two realms. A 6BR may implement a proxy that can convert the 6IoT technologies, such as CoAP, to Internet technologies, for example HTTP. However, such proxies may not ensure E2E security; for example, 6BR proxies cannot ensure E2E security if Transport Layer Security (TLS) is used on the Internet side and DTLS is used in the 6LoWPAN network.

2.2 DTLS and CoAP

DTLS [5] is a variant of the TLS protocol that is designed to run over UDP. DTLS is a mandatory part of CoAPs. It borrows the Handshake and Record protocols from TLS. The Record protocol encapsulates and secures other protocols, such as the *Handshake*, *Alert*, *ChangeCipherSpec*, and application data. Due to the unreliability of the UDP protocol, DTLS incorporates mechanisms to retransmit and assemble packets. The DTLS Handshake protocol is a complex process and exchanges different messages to negotiate the cryptographic cipher suites, compression methods, security keys, certificates, etc. Once the Handshake protocol is completed the application can send secure messages using the Record protocol and negotiated keys and cipher suites. The Record protocol ensures the freshness, integrity, and confidentiality of the application data.

The Constrained Application Protocol (CoAP) [2] is a new web protocol. It is a subset of the HTTP protocol optimized for Machine-to-Machine (M2M) applications running on resource-constrained nodes. CoAP works over the UDP protocol where message exchanges are asynchronous, in contrast to the HTTP protocol that sends synchronous messages. CoAP borrows HTTP features such as Uniform Resource Identifiers (URIs) but uses packed binary representations, and uses only GET, POST, PUT and DELETE messages in a request/response model. The reliability in CoAP is achieved through *confirmable* messages that use acknowledgments. Secure CoAP (CoAPs) uses DTLS to secure CoAP messages. If a URI specifies the CoAPs protocol ($coaps : //myIP : port/resource.xml$), DTLS protocol processing is performed before the CoAP message is passed to the UDP layer. At the receiving end, the DTLS protocol is placed between the UDP and CoAP layers.

2.3 Android-Enabled Smartphones

Android is an open source operating system that is designed primarily for smartphones. Android-powered smartphones are abundant in number, available in different cost range, and actively in production by different vendors. Due to wider range and availability, smartphones in general and Android-powered phones in particular have a huge potential to be used in the 6IoT; we discuss potential applications in Section 4. Different CoAP implementations exist for Android phones to enable communication with WSNs/6LoWPANs. Also, there exist DTLS implementations in the C programming language. However, to the best of our knowledge no DTLS/CoAPs implementations exist for an Android device nor does there exist full CoAPs support for any platform. Android applications are developed using Java APIs for Android. Java Native Interface (JNI) that enables the integration of C language code in Java could be used in Android; however, it increases the complexity and decreases the performance of Android applications.

3 INDIGO: CoAPs for the Android OS

We present INDIGO, a CoAPs support for the Android OS. In this section we elaborate the capabilities of INDIGO and the description of INDIGO client and server.

3.1 INDIGO Capabilities

We implement the full DTLS protocol with Record, Alert and Handshake protocols, and integrate it with the CoAP protocol. INDIGO is a complete client/server system that enables CoAPs support in the Android OS and can also be used in standard computers. INDIGO supports all cryptographic cipher suites which are standardized in the CoAP protocol [2]. Recall that the CoAPs protocol is a CoAP protocol secured with DTLS. The DTLS protocol in INDIGO is standard compliant [5] and supports certificate-based mutual authentication between DTLS client and server. INDIGO has following capabilities:

- Applications can seamlessly send/receive reliable and unreliable CoAP or CoAPs messages; INDIGO exports these capabilities to the applications and differentiates between CoAP and CoAPs. For example, to securely access a dummy resource *stockholm_temp.xml* an application can use *coaps://myIP:port/stockholm_temp.xml*, and the underlying INDIGO secures the communication links and performs necessary tasks which are described in Section 3.2 and 3.3.
- INDIGO can act as a CoAPs client or a CoAPs server on an Android device.
- It supports the standardized DTLS Handshake protocol with retransmission mechanisms when a client or server does not receive the intended response messages within timeouts.
- The DTLS Handshake protocol supports certificate-based mutual authentication and uses the Elliptic Curve Digital Signature Algorithm (ECDSA) for asymmetric encryption/digital signature. The key exchange protocols supported during the Handshake protocol are Pre-shared Key (PSK), Elliptic Curve Diffie Hellman (ECDH), and Elliptic Curve Diffie Hellman Ephemeral (ECDHE). ECDH has a fixed DH key which means that one side during the handshake process does not change the key for consecutive handshakes.

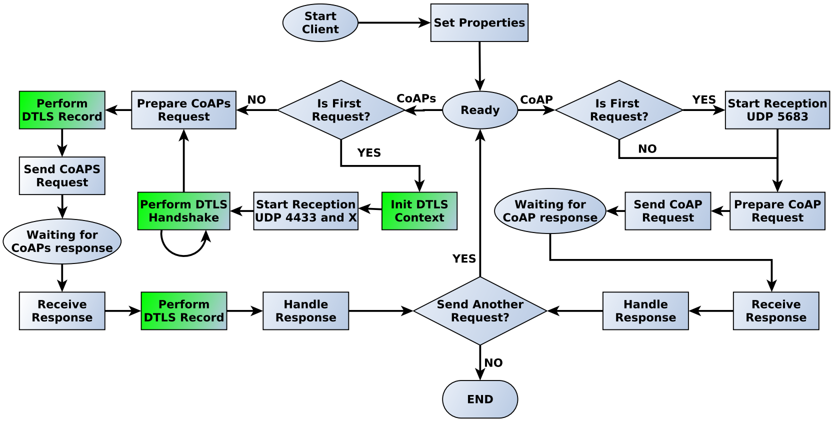


Fig. 1. States and flows when an application uses INDIGO Client to send/receive CoAP or CoAPs requests

On the other hand, Ephemeral mode generates distinct Diffie Hellman key for every handshake which ultimately provides forward secrecy; however, it is less efficient than ECDH as it requires more cryptographic operations.

- The DTLS Record protocol supports Counter with Cipher Block Chaining MAC (CCM) mode for confidentiality and integrity of CoAP messages. For the confidentiality of CoAP messages, the Advanced Encryption Standard (AES) with key size of $128 bits$ (AES-128) or with $256 bits$ (AES-256) can be used in Counter mode in CCM; and for integrity, the Cipher Block Chaining (CBC) mode in CCM is used with the same AES-128 or AES-256 protocol where the most significant $64 bits$ of the last encrypted block are used as Message Authentication Code (MAC).
- SHA-256 is supported and used to generate or verify the hashes of all DTLS messages as specified in the DTLS protocol. Also, SHA1 is used in the CertificateVerify message to calculate and verify the hash of all prior messages. INDIGO does not include ClientHello and HelloVerifyRequest messages in the hash calculation as specified in the DTLS protocol.
- The above capabilities make INDIGO compliant to the CoAP protocol [2] as it supports the following mandatory cipher suites, `TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8` and `TLS_PSK_WITH_AES_128_CCM_8`.

3.2 INDIGO Client

An application on one machine can establish a secure connection with a remote application, and can act as an INDIGO client or server. When INDIGO runs as a client it can be used to request CoAP or CoAPs resources; Figure 1 shows the complete flow and different states of the INDIGO client. As a client, INDIGO starts with setting necessary properties for CoAP and DTLS such as port number

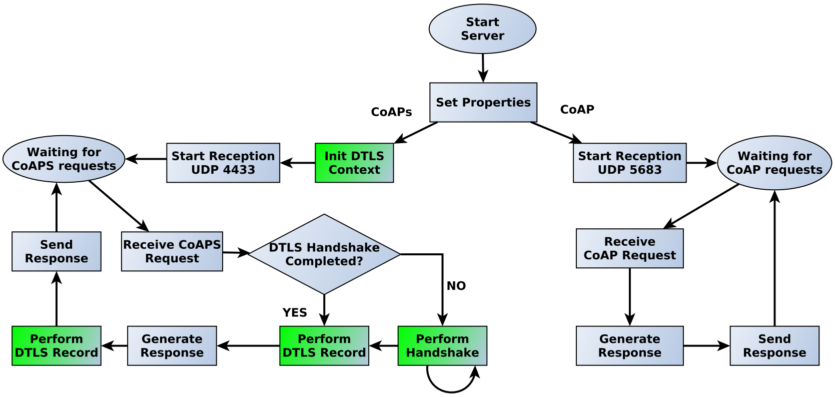


Fig. 2. States and flows when an application uses INDIGO Server to receive and respond to CoAP or CoAPs requests

and timeout. Then based on the protocol in the URI it either starts CoAP or CoAPs processing. If an application decides to use CoAP for a request, INDIGO prepares the CoAP request, sends it, and goes to waiting state to wait for the CoAP response. If it is the first CoAP request since the client started, INDIGO starts the reception process for the CoAP response. Upon reception of the CoAP response INDIGO processes it, returns the result to the application, and lets the application decide whether it wants to send another CoAP or CoAPs request.

If an application decides to use the CoAPs protocol for a request INDIGO creates a CoAPs request, performs DTLS Record protocol processing to add confidentiality and integrity to the message, sends the CoAPs request, and waits for the response. If it is the first CoAPs request since the client started, INDIGO initializes the DTLS context, starts the reception process for the Handshake responses at port 4433 and for the CoAPs responses at port IANA_TBD_PORT, and performs the complete DTLS Handshake protocol. The CoAPs port is not yet assigned by IANA [2]; the actual CoAPs port should later replace IANA_TBD_PORT. Upon reception of the CoAPs response INDIGO verifies the integrity of the messages and decrypts the confidential data using the Record protocol.

3.3 INDIGO Server

An application can use INDIGO as a server to respond to CoAP or CoAPs requests; Figure 2 shows the complete flow and different states of the INDIGO server. To this end INDIGO sets necessary properties for CoAP and DTLS such as CoAP/CoAPs port number, timeout, DTLS port, if it needs to act as a client or sever; and initializes the DTLS context in order to retrieve the certificates and keys used for encryption and authentication. It binds CoAP to port 5683, CoAPs to port IANA_TBD_PORT, and DTLS to port 4433. Then it goes to waiting state to listen for CoAP/CoAPs requests. If it receives a CoAP request it simply retrieves the requested resources, generates the corresponding response, and sends it to the client. Then it listens for new CoAP requests. On the other hand if the INDIGO server receives a CoAPs request it ensures that the handshake performed earlier is still valid and/or performs a full handshake with the client by sending a *Hello Request* message [5] [6]. If needed, it performs DTLS Record protocol processing to decrypt and verify the CoAPs request, generates the response and sends it to the client. Then it listens for new CoAPs requests.

4 Applications of INDIGO

Current smartphones are versatile devices with processing and storage capabilities though slightly less but similar to standard computers; a smartphone is a mini computer. However, unique features such as physical portability, close human interaction, sensing capabilities with having accelerometer, proximity, gyroscope, camera, sound, compass, GPS, Wi-Fi, GPRS/3G/4G, Bluetooth, even Near Field Communication (NFC), enable smartphones to be used in an enormous number of applications and scenarios. In the context of 6IoT a smartphone can be used as a sensing device, a 6LoWPAN Border Router (6BR), or an actuator or controller. Of course it can also be used as a typical computer to access/provide data to other Internet hosts and WSNs/6LoWPANs.

Smartphone as Sensor. In urban areas smartphones are the enabling technology for opportunistic and participatory urban sensing [7][8]. Due to the large availability and vast capabilities smartphones can be used in traffic congestion control and management, security and emergency services, access control, NFC payments, location detection, etc. Though in all these scenarios smartphones are the actual sensing devices they may complement these applications with the input from typical sensors that have limited resources. Recall that the 6IoT is an extremely heterogeneous network where many devices are resource constrained and expected to use standardized CoAP/CoAPs protocol. Therefore, it is important that all devices, in order to communicate and provide E2E security, should use the same secure protocol.

Smartphone as 6BR or Sink. We envision it beneficial to use a smartphone as a 6BR to connect 6LoWPAN networks or as sink to connect WSNs with the Internet especially when there is no wired infrastructure. In developing countries such as Pakistan and India the mobile coverage spans to more areas than the wired Internet access. Also, in remote areas such as forest, glaciers, deserts, mountains, etc. there is no wired Internet. Android-enabled smartphones have quite cheap models available that can be used as a 6BR in the 6IoT setup or a sink in traditional sensor networks to connect 6LoWPANs/WSNs deployed in the remote locations to the back-end servers. The sensors in 6LoWPAN networks can establish E2E secure connections with smartphones using the CoAPs protocol; or they can even establish these secure connections with the hosts on the Internet through the smartphone. In that case the phone only acts as a 6BR but cannot see the content of messages. The potential applications where a smartphone can be used as 6BR/router can be patients surveillance and monitoring where doctors can use smartphones to get latest patient information from the body area sensors network, military applications, flood monitoring and response system, glacier monitoring in the Himalayas region, animal tracking and monitoring, etc.

Smartphone as Actuator and/or Controller. The typical use of smartphones in the 6IoT context is to act as an actuator and/or controller. For example, in a smart home application a smartphone can be used to turn on and off thermostats or any other appliances. It can be used as interface to display and/or manage electricity consumption in smart grid/meter/plug applications, and in any 6IoT application where human interaction is needed or make it more useful smartphones are a valid solution. There are already sensor devices available such as *ube*'s smart devices[1] which use the Android OS as the main operating system in the sensor. *ube* uses a 32-bit ARM processor that runs the Android OS with a full IP stack and communicates over Wi-Fi by connecting to a local wireless router. They use smartphones as an integral part of the whole system which controls and actuates the sensors.

In all of these applications and scenarios security is one of the main requirements; imagine if someone could turn on your thermostat or can turn off your lightening system.

5 Implementation

INDIGO provides DTLS client and server implementations in the Android/Java programming language and integrates them with the CoAP protocol. Currently INDIGO borrows CoAP protocol capabilities from Californium[2]- a Java implementation of CoAP; and with little effort it can be integrated with any CoAP implementation favorably in Java. INDIGO's DTLS implementation is self-containing and designed as a standalone module that can be used by different applications even without CoAP. However, as our focus is to enable secure CoAP (CoAPs) we also provide a full integrated (CoAP + DTLS) system and use it in our evaluation. INDIGO's DTLS module communicates with the CoAP protocol through Java's publish-subscribe pattern using multiple threads which allows *simultaneous* and asynchronous operations. In this way more applications can use the same implementation by registering as *observer* when required. If the application desires a synchronous operation it is always possible to serialize the subscriber's method.

Java Cryptography Extension (JCE) APIs in plain Java neither provide DTLS APIs nor full certificate-based cryptography. Therefore, in addition to JCE, we also use cryptographic APIs from SpongyCastle[3] to develop INDIGO. We implement the full DTLS protocol from scratch; however, we borrow AES, SHA, and ECC APIs from JCE. We also develop CCM_8 mode from scratch. We plan

[1] `http://www.myube.co/`

[2] `http://people.inf.ethz.ch/mkovatsc/californium.php`

[3] `https://github.com/rtyley/spongycastle`

Table 1. Total time of INDIGO Handshake protocol with CPU time of individual Handshake flights inside a smartphone

Smartphone as DTLS client			**Smartphone as DTLS server**		
Process	Avg Time (ms)	Std Dev	Process	Avg Time (ms)	Std Dev
Full Handshake	3387.2	393.3	Full Handshake	4881.4	489.6
Flight 1	20.6	6.0	Flight 2	2.4	21.0
Flight 3	1.0	0	Flight 4	698.6	40.3
Flight 5	300.4	24	Flight 6	3.2	1.2

to publish INDIGO as open source. Though INDIGO is designed primarily for the Android OS it can be used in standard computers. In our evaluation we run INDIGO in both a PC and in a smartphone.

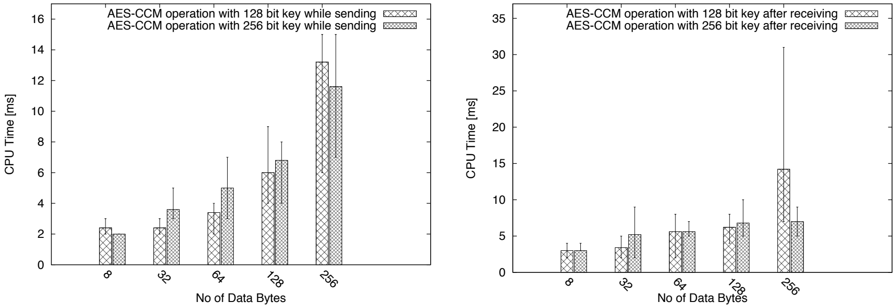
6 Evaluation

In this section we evaluate the overhead of the Handshake and Record protocols in INDIGO comparing the CPU usage of different cryptographic algorithms used in the DTLS Record protocol, total time of the Handshake protocol and the CPU time of individual flights in Handshake, and system-wide round trip times of CoAP and CoAPs requests. We cannot compare our CoAPs implementation against other solutions since there are no other CoAPs implementations available.

6.1 DTLS Handshake Protocol Overhead

Unlike the Record protocol, the Handshake protocol is not performed every time a client or a server wants to exchange messages. Communication end points perform the full Handshake protocol only when a new UDP connection is established or when a client or server wants to renegotiate an already established connection.

In our first experiment we measure the time required to perform a full Handshake protocol *(i)* when a smartphone acts as an INDIGO client and *(ii)* when a smartphone acts as an INDIGO server. The experimental setup consists of a smartphone and a standard computer connected through Wi-Fi. One device acts as a client and the other as server. Table 1 shows the total time spent on the Handshake when the smartphone acts as a client and a server. The total Handshake time in both cases should be equal as the same operations (total flights) are performed. However, it differs because the standard computer we use for evaluation is more powerful than the smartphone (Google Nexus with Android 4.0). The total time is effected by unpredictable Wi-Fi and Android internal process management and CPU scheduling. In order to get clearer picture of the actual *Handshake* protocol overhead, we measure the overhead of each Handshake flight [5] when it is performed inside a smartphone. Table 1 shows that the flight 4 and 5 are processing intensive flights; these flights consist of key exchange protocols and perform asymmetric cryptographic operations.



(a) AES-CCM operations with 128*bits* key performed before sending CoAPs message.

(b) AES-CCM operations with 256*bits* key performed after receiving CoAPs message.

Fig. 3. The cryptographic operations in the Record Protocol show that different key sizes have similar overhead

6.2 Cryptographic Overhead in DTLS Record Protocol

The Record protocol ensures the confidentiality and integrity of application data using AES in CCM mode. The overhead of AES CCM mode is added in each datagram on both the sending and receiving ends. Hence it is important to know how much time a CPU spends on processing cryptographic operations. We use different key sizes. As shown in Figure 3 the overhead of AES with different key sizes is almost same considering that there is high standard deviation and smartphones are not resource constrained devices.

6.3 Round Trip Time for CoAPs Messages

Once the secure connection is established by the Handshake, nodes only execute the Record protocol to secure the subsequent messages. In this experiment

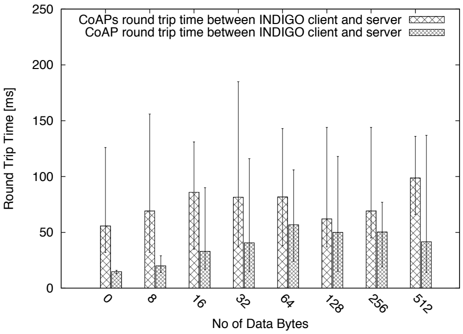


Fig. 4. The round trip time for CoAPs secured with the Record protocol is, as expected, higher than for the CoAP protocol

we measure the round trip time (RTT) which is the time from the creation of a CoAP/CoAPs request until the CoAP/CoAPs response is received and processed. The intermediate steps are shown in Figure 1 and 2. Figure 4 shows the RTT for a CoAPs request and compares it with a CoAP request. Recall that the high standard deviation is because of unpredictable Wi-Fi and Android internal process scheduling as many processes run inside an Android device.

7 Related Work

We are not the first to argue that the E2E security is necessary for the 6IoT, but we are the first to enable secure CoAPs communication between the constrained devices in the 6LoWPANS and smartphones. To the best of our knowledge currently there is no CoAPs support available for any platform. However, there are CoAP implementations available for different platforms such as Californium, jCoAP[4] and Earbium[5]. Also, DTLS support is available in the C language which is provided by OpenSSL[6], CyaSSL[6] GnuTLS[6]. In constrained devices CoAPs can be provided, for example, by integrating Earbium[5] and DTLS implementation in OpenSSL.

Brachmann et al. [9] elaborate the practical security issues in CoAP/6LoWPAN networks and the feasibility to use DTLS for E2E security and secure multicast. Kothmayr et al. [10] investigate the use of Trusted Platform Module (TPM) to provide DTLS in 6LoWPAN networks where they rely on hardware support for the RSA algorithm. We have previously presented solutions to compress DTLS to make it feasible for constrained devices [11]. Communication in the 6IoT can be secured at lower layers by, for example, using IPsec [12] or 802.15.4 security [13].

8 Conclusion

In order to securely connect and integrate smartphones in the 6IoT it is necessary to use standardized security solutions. CoAPs, the standardized secure web protocol for the 6IoT, is not yet available in smartphones. Towards this end, we have designed, implemented, and evaluated CoAPs for the Android OS. We have shown that smartphones with CoAPs capabilities can be used in many applications and hence we expect that CoAPs will play an important role in the future 6IoT. In the future, we plan to implement CoAPs for constrained devices and will evaluate the full 6IoT system consisting of sensors and INDIGO-powered smartphones.

Acknowledgements. This work has been partly performed within the SICS Center for Networked Systems (CNS), and partially funded by CALIPSO (FP7-ICT-2011.1.3-288879).

[4] http://code.google.com/p/jcoap/

[5] http://people.inf.ethz.ch/mkovatsc/erbium.php

[6] http://www.openssl.org, http://www.yassl.com,
http://www.gnu.org/software/gnutls

References

1. Kushalnagar, N., Montenegro, G., Schumacher, C.: IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals. RFC 4919 (August 2007)
2. Shelby, Z., Kartke, K., Bormann, C., Frank, B.: Constrained Application Protocol (CoAP). draft-ietf-core-coap-12 (October 2012)
3. Hui, J., Thubert, P.: Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks. RFC 6282 (September 2011)
4. Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, J., Alexander, R.: RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. RFC 6550 (March 2012)
5. Rescorla, E., Modadugu, N.: Datagram Transport Layer Security Version 1.2. RFC 6347 (Proposed Standard) (January 2012)
6. Dierks, T., Rescorla, E.: The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246 (Proposed Standard) (August 2008); Updated by RFCs 5746, 5878, 6176
7. Campbell, A., Eisenman, S., Lane, N., Miluzzo, E., Peterson, R., Lu, H., Zheng, X., Musolesi, M., Fodor, K., Ahn, G.: The rise of people-centric sensing. IEEE Internet Computing 12(4), 12–21 (2008)
8. Cuff, D., Hansen, M., Kang, J.: Urban sensing: out of the woods. Communications of the ACM 51(3), 24–33 (2008)
9. Brachmann, M., Garcia-Morchon, O., Kirsche, M.: Security for practical coap applications: Issues and solution approaches. In: Proc. of the 10th GI/ITG KuVS Fachgespraech Sensornetze, FGSN 2011 (2011)
10. Kothmayr, T., Schmitt, C., Hu, W., Brunig, M., Carle, G.: A dtls based end-to-end security architecture for the internet of things with two-way authentication. In: 2012 IEEE 37th Conference on Local Computer Networks Workshops (LCN Workshops), pp. 956–963. IEEE (2012)
11. Raza, S., Trabalza, D., Voigt, T.: 6LoWPAN Compressed DTLS for CoAP. In: Proceedings of the 8th IEEE International Conference on Distributed Computing in Sensor Systems (IEEE DCOSS 2011), Hangzhou, China (May 2012)
12. Raza, S., Duquennoy, S., Chung, A., Yazar, D., Voigt, T., Roedig, U.: Securing communication in 6lowpan with compressed ipsec. In: 7th International Conference on Distributed Computing in Sensor Systems (DCOSS 2011), Barcelona, Spain (2011)
13. Raza, S., Duquennoy, S., Höglund, J., Roedig, U., Voigt, T.: Secure Communication for the Internet of Things - A Comparison of Link-Layer Security and IPsec for 6LoWPAN. In: Security and Communication Networks. Wiley (January 2012)

Author Index