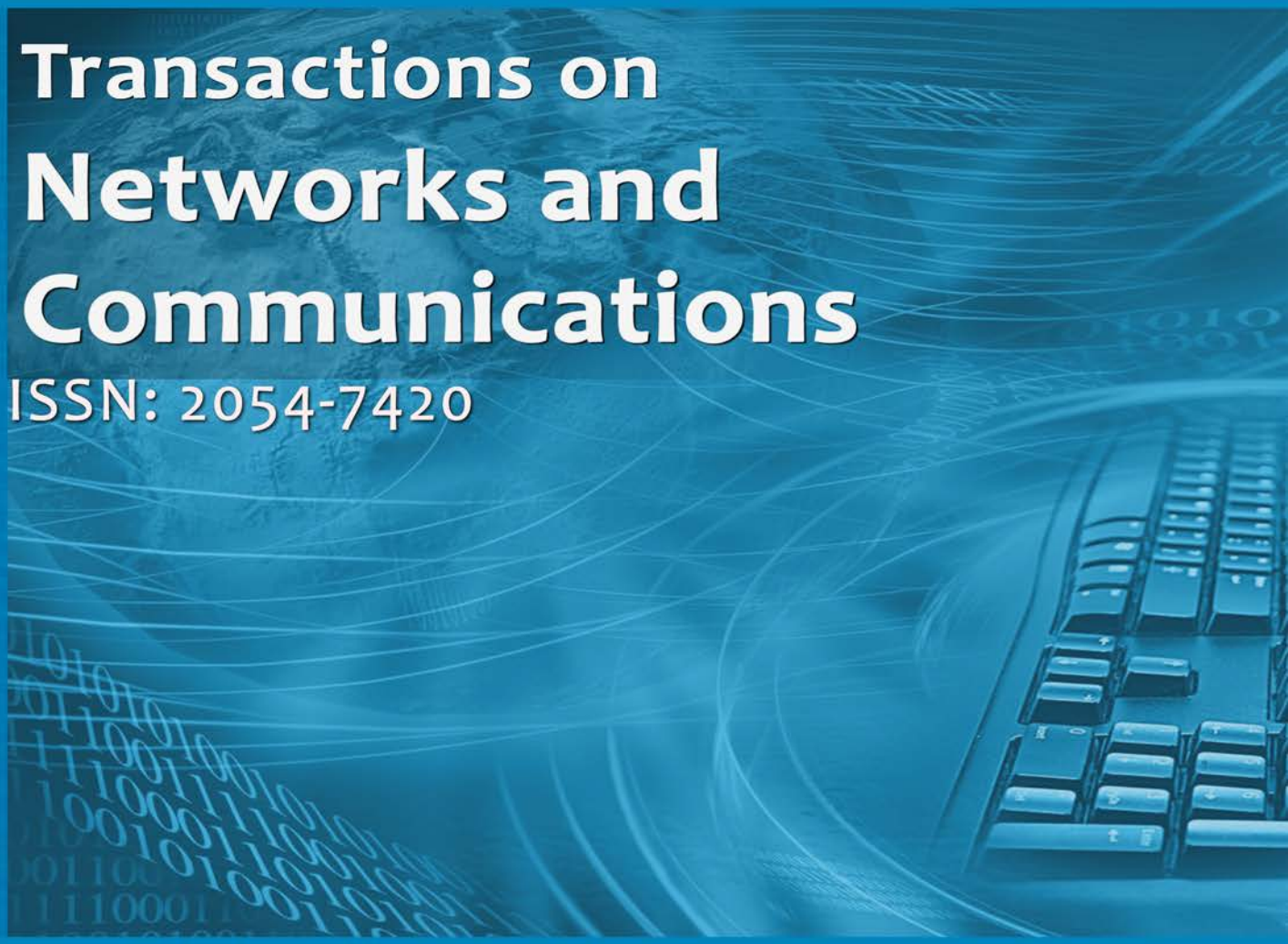
Volume 3. Issue 3 - June 2015

Transactions on Networks and Communications

ISSN: 2054-7420



Society for Sciences and Education - United Kingdom

TABLE OF CONTENTS

EDITORIAL ADVISORY BOARD

DISCLAIMER

All the contributions are published in good faith and intentions to promote and encourage research activities around the globe. The contributions are property of their respective authors/owners and the journal is not responsible for any content that hurts someone's views or feelings etc.

TNC Transactions on Networks and Communications
SOCIETY FOR SCIENCE AND EDUCATION UNITED KINGDOM
VOLUME 3, ISSUE 3
ISSN: 2054 - 7420

Radio Frequency Identification upon Near Field Communication and Far Field Communication for Next Generation Wireless Network Infrastructures

[1]Gowher Mushtaq, [2]Shashank Singh, [3]Neeraj Kumar Tiwari, [4]Seemab Rasheed, [5]Yogesh pal and [6]Kavita Srivastava
Shri Ramswaroop Memorial University Lucknow India
[1]gowhermushtaq@ymail.com; [2]shanky197@ymail.com; [3]neeraj.cs@srmu.ac.in;
[4]seemab.singer@gmail.com; [5]er.yogeshpal15@gmail.com; [6]wwwbkb@rediffmail.com

ABSTRACT

The electromagnetic field that outlines the RFID antenna can be divided up into two portions – Near-field and Far-field. Near Field Communication (NFC) and Far-Field communication (FFC) both are the most emerging wireless short-range communication technologies, both are based on existing standards of the Radio Frequency Identification (RFID) network framework. In collaboration with NFC-efficient next generation smartphones it authorizes automatic application frameworks for contact less connections, in different exceptional utilities for future generation smartphone payment and over-the air ticketing. The principle aim of current study is to explain basic characteristics and benefits of the wireless short- range technologies like (RFID, NFC, and FFC) and analogy between them to classify modes of operation and to present various illustrations. NFC mechanism, applications and FFC with possible future or Next Generation scenarios will be analyzed. Finally, this study provides the fundamental security concerns; challenges and present conflicts will be investigated in order to achieve the efficiency in Next Generation Network Infrastructures.

Keywords: Electromagnetic Field, RFID, NFC, FFC, Smartphones, Next Generation

1 Introduction

According to the study work of Roy Want in [1], "Radio Frequency Identification Technology (RFID) has been developed from complexity into main stream applications that let us help to rate the manipulating of assembled figures and stocks facts". Accordingly, Bar code which is probably the best performer in transmitting sequence of productions and organizational warehouses in the future generation network infrastructures. However, RFID is exchanging bar code technology and be entertained by one of the crucial advantage of being independent of line of sight problems and scanning the objects from a distance. It anticipates the skeleton of amplified visibility, updated tabulation management and decreased labor levels. According to the latest information standards, Wal-Mart has been one of the leaders in the large scale adoption of RFID technology [1]. RFID tags have a memory capacity of 16 - 64 Kbytes which is far more than the barcodes (1-100 bytes) [1] and can store additional data such as manufacturer name and product specifications.

The initial step for the development of RFID was during World War II, when the British manipulates it to identify whether planes belonged to "friend or enemy". Some technical problems resulted in the gunning down of allied planes and since then the use of RFID was limited to Defense and armed forces industries due to the cost factors. New advancements in science and technology have enabled usage

DOI: 10.14738/tnc.33.1167
Publication Date: 9th May 2015
URL: http://dx.doi.org/10.14738/tnc.33.1167

in commercial applications. Large institutions, such as the US Department of Defense, have since implemented RFID which is now spreading to other organizations and Multi-National companies [1]. Wal-Mart is the world's second biggest user of RFID and investing significant resources to develop its highly efficient applications. RFID technology operates at multiple frequencies counting low, high and ultra-high. The frequency that is being carried out discovers the distance in which RFID tags can be measured, how many tags can be interpreted at one time, how fast these tags are calculated, and how can application framework will influence its performance.

When making a choice between two technologies, it is significant to acknowledge their separate program propriety, implementation abilities, intensities, and deficiency. By surveying the different utilizing principles and future habitat affects, we should make a literate conclusion advance to implementing any path and explore technology. One more satisfaction, when deciding the proper frequency for a communicating application is the quantity of electromagnetic interference (EMI) and sensitivity to exterior programmer components i.e. water, metal, Muscularity, evaporation, or any other data influence, inversion, etc. Within the last few years a communicative technique has appear to emerge integrating computational cognition into different kinds of objects of our day to day life and permitting we people to constantly connect with those objects. The proposal is to positively connect virtual information to objects of the material world and therefore providing global computing. Comparable to the abstraction of network universality is the term 'Internet of Things' introducing to objects of daily use being verifiable, measurable and even virtually connected via an internet-like framework [2].

A leading designer for this perception is the technology of Near Field Communication (NFC) that provides the possibility of linking virtual information between physical devices via adjacency. Virtually all object or place can be assembled with a NFC tag and thus provide proximate identification and useful related information to a nearby user of a smart device, like a tablet computer or a smart phone [2].

The intention of this study is to summarize opportunities provided by Radio Frequency Identification combining the technology of Near Field Communication and Far Field Communication with the capabilities of modern smartphones. It will point out recent trends and present application scenarios, but also address challenges and obstacles that might occur when trying to make NFC suitable for the mass market.

First, it will be necessary to provide a basic technical understanding of Near Field Communication. The first chapter will thus roughly explain the functionality of NFC and its underlying technique of Radio Frequency Identification (RFID). Its characteristics will be described and necessary hardware components and different modes of operation will be specified. Furthermore, examples for mobile ticketing will also be discussed as well as possible applications for medical assistance and for other market segments. The final part of this paper will deal with potential security issues and other challenges mostly related to present conflicts due to clashing interest of different groups of stakeholders. Addressing this topic is essential for eventually providing an outlook for the future development and estimation for the expected prospect of success in the context of RFID with respect to Near Field Communication and Far Field Communication.

2 Related work

The NFC technology was launched in 2004, when it was regulated by NFC forum. NFC forum act as an authority to define NFC standards and specifications. It is also responsible for technology's further improvement. NFC standards are defined in ISO 18092 and in its counterpart ECMA-340 standard. The technology of NFC and FFC has been yielded from RFID (Radio frequency Identification) and is also consistent with this. However, NFC technology is being observed RFID‟s apparent and RFID is its scion. The aspects drafted for RFID technology i.e. RFID tags or devices are emerged with standard ISO 14443 and are also acceptable to function with NFC technology. Besides, NFC devices are also well matched with RFID tags from MIFARE and FeliCa brands, developed by Philips and Sony respectively [3]. In this bodywork, the survived literature has been classified into theoretical fields and applications. The imaginary areas include security, technology, organization, and privacy.

RFID tags fall into two categories, active tags, which consists an internal energy authority, and passive tags, which gathers energy from the wave of an external reader. A passive tag consists of a microchip enclosed by a printed antenna and some type of encapsulation, plastic laminates with viscous that can be connected to a product or a small glass bottle for convention. The tag reader powers and communicates with passive tags. The tag's antenna organizes the process of ID transfer and energy capture. A tag's chip frequently occupies data to analyze a sole product, the product model and manufacturer.

NFC is a short-range wireless communication technology that is placed on authorized and sophisticated standards in the field of RFID and smart cards. RFID, which has been made known in the 1970s, recognizes robotic description and data transfer via electromagnetic radio signals consistently by means of an active reader that is connected to a source of energy and a passive electronic tag that is a transponder receiving its power from the reader by magnetic induction.

3 Research Methodology

The fundamental motive of this study is to explain basic characteristics and benefits of the underlying technologies (RFID, NFC, and FFC) and the comparison between them, to classify modes of operation and to present various illustrations. NFC applications, mechanism and FFC with possible future or Next Generation scenarios will be analyzed in this paper. Finally this study provides the fundamental security concerns; challenges and present conflicts that will be investigated in order to achieve the efficiency in Next Generation Network Infrastructures with respect to Radio Frequency Identification.

3.1 RFID (Radio Frequency Identification)

Radio Frequency Identification (RFID) is a form of automatic identification technology (auto ID). Auto ID is characterized by data forms that are machine readable. Other classification of Auto ID contain electronic article surveillance (EAS) safety tags, bar codes, magnetic stripes, optical character recognition, optical character group (OCG) etc. These technologies can be additionally identified by those that need contact in order to be read (magnetic stripes), and those that do not (such as, bar codes, EAS, OCG, RFID). RFID differs from bar codes and most other contactless auto ID data forms in that the data can be read without a direct line of sight to the reader. Additionally, read intervals can be comparatively high (feet versus inches). Utilizing RFID measures that:

- Compact human embarrassment is needed for the proper information or data improvement.
- Improvement can be fast-moving.
- With the perfectly installed and influenced system, data represented through RFID is more authentic and obtained at lower costs.

This high-level standard of automation makes RFID self-confident to be an auto ID technology that could change the way in which information is collected and utilized.

Presently, RFID is utilized in various applications, oscillating from computerized installments for tracking goods during the supply chain. The utilization of RFID technology in closed-loop systems is as powerful as applications for chasing goods. In 2008, the quantity of RFID chips used in different closed-loop, mass movement tickets and cards was about balanced to those utilized in open- supply chain goods recording. A Radio Frequency Identification (RFID) system consists of readers (also called interrogators) and tags (or transponders). A classic system has a few readers, either static or mobile, and various tags, which are connected to objects, such as bottles, platforms, cartons, etc. A reader broadcasts with the tags in its wireless domain and gathers information about the objects to which tags are connected. Depending upon their working theory, tags are categorized into three headings:

- Passive,
- Semi-Passive, and
- Active.

A passive tag is the least sophisticated and consequently the cheapest. It has got no interior energy maternity but in order get better transmission results passive tag uses the electromagnetic field (EM) transmitted by a reader to power its interior router. It acts on “back-scattering” not on a transmitter to transmit data reverse to the reader. A semi-passive tag has got its own energy source but it has got no transmitter and also utilizes back-scattering. While as in comparison to both of the two tags, an active tag has both internal power supply and an on-tag transmitter.

A simple Example of Closed Loop System:

An example of a closed loop system is the disaster expulsion system for the humor of Texas. The Texas regional jurisdictions along with National companion, provides consolation to common people that are requesting for the help to move out from the awaiting disaster (cyclones are the common example). The efforts that are attached with the disaster were historically efficient, but planning for understanding the evacuation progress, shelter, getting information’s about the individual with their location and being able to respond to concerned relatives required great effort including calling many shelters sites and hospitals to locate family members.

In 2008, Texas put into effect a spontaneous RFID-based Special Needs Evacuation Tracking System (SNETS), developed by LLC, Radiant RFID, to help manage the overall evacuation. Almost every person who needs aid can choose to wear the RFID wristband. The particular wireless wristband is made up of a unique number, bar code and electronic code that associate to the person’s private data in a secure database. The wristband is read at expulsion bus conversion points, boarding sites, and final shelter locations. People like friends; relatives etc. can contact a 211 or 800 number which is printed on the band and request that the displaced person can contact them. State officials then locate the displaced person in the SNETS database, and notify the migrant in the inquiry. The wristband interference system certifies the messages delivered to the right expulsion location’s electronic message center, and gets permission for recovery communications. The particular system does not acknowledge the displaced person’s location (only that person which is displaced from her/his location can expose his/her position, through a message).

With the speed and reliability of RFID tag reads, this system is effective during the urgent pace of evacuating large numbers of people. More than 40 thousand wristbands were issued and deployed in 2008 for Hurricanes Ike and Gustav in Texas.

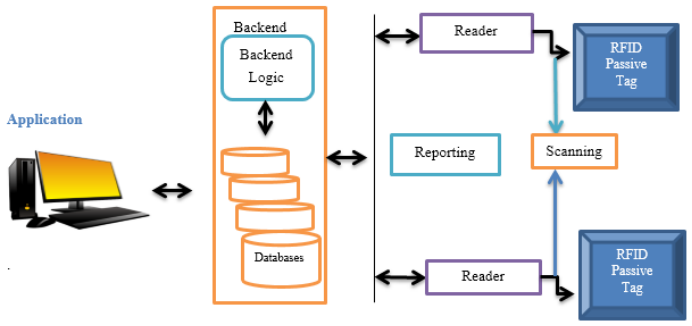


Figure 1: A simplified RFID System

In RFID, reader and some other particular tags in general are having a little use. The healing of a sequence number does not provide much information to the user and nor does it help to keep record of items in a management group. The absolute energy of RFID arrives in consolidation with a tail end that stores extra information like confession about the products, when and where a positive tag was investigated. Furthermore, the RFID system has been described through structure as explained in figure 1. RFID readers firstly, scan tags and then transfer the information to the backend. The backend in normal form consists of a database and a well-defined application interface. When the backend gathers some additional source or what we can say information that particular information is stored in the database for further processing, and if required it implements some computation on associated disciplines. The application brings back the data or information from the backend. Through various scenarios, the application is assembled with the reader itself. An example of this particular scenario is the consistent point in a shopping center (Note that the specific example uses barcodes rather than RFID tags after all they are highly accepted, in spite of, the system would act in absolutely the same manner if tags were utilized). The application uses the copied identifier to take care of the current cost when RFID reader scans the barcode. In inclusion to that, the application backend also transfers premium information for certified commodities. The backend also reduces the sum of feasible commodities of that type and alerts the manager if the quantity falls below a sure verge.

3.2 RFID classification

The classification of Radio Frequency Identification is showing below through a diagram

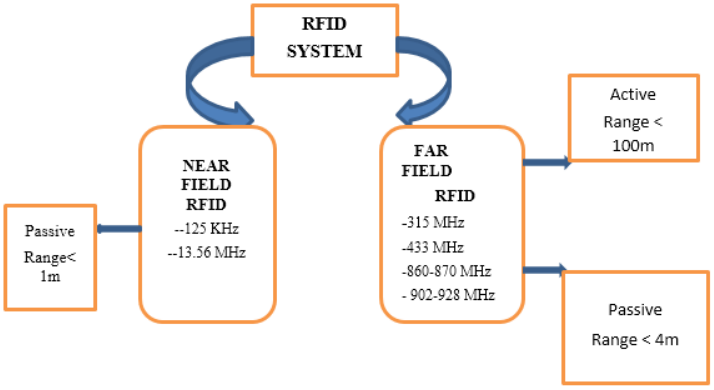


Figure 2. Showing the Classification of RFID

3.3 Brief History

The concept of communication using reflected radio energy is quite old and dates back to the origin of radar technology. Many developments in the early 20th century applied radio back-scatter. For example, the Identify-Friend or Foe (IFF) transponder developed by British was used by the allies in World War II for identification of friendly aircraft. It relied on passive radar reflectors, tuned to the home radar frequency, which made a friendly aircraft much brighter to home radar than an enemy aircraft.

Among the earliest and significant works related to RFID is the continuous time modulation of reflected signals, published by Stockman in October 1948 [5]. While he was working at the Air Materiel Command in Massachusetts, he launched a device and designed it in the way which modulated human voice on reflected light signals. The decagons of the 1960s and 1970s were marked by the research community's interest in RFID. An early breakthrough of this period was a passive RFID transponder developed and patented by Richardson in July 1963. The device could couple and rectify energy from an interrogator's EM field and transmit signals at a harmonic of the received frequency. Later in the decade, Vinding developed a simple and inexpensive interrogator-transponder system based on inductive coupling, which was granted a U.S. patent in January 1967[5]. The transponder used repetitive tuning or loading of its antenna circuit at a rate characteristic of the particular transponder under interrogation. Koelle, Depp and Freyman, while at Los Alamos Scientific Laboratory (LASL) in northern New Mexico, introduced the novel concept of transponder antenna load modulation as a simple and effective way for backscatter modulation in August 1975.

The first commercial application of RFID — Electronic Article Surveillance, was introduced by associations such as Sensormatic, Kongo, and Checkpoint in the late 1960s. Commercialization picked up in the 1980s and 1990s with varying interest in different parts of the universe. Fundamental interests in the United States constitute office connection and transportation, during European countries were interested in short-range systems for tracking animals, industrial and business applications and electronic toll-collection. The first RFID-based toll-collection system became practical in Ålesund, Norway in October 1987. The development in commercial use of RFID, the organization of RFID suggests a requirement for assumptions, which assist to numerous standardization activities in the 1990s. Most of these were conducted by the International Electro-technical Commission (IEC) and International Standards Organization (ISO).

ISO, an international organization upon which 157 countries belong, develops industry-wide standards in a series of greens. Accordingly, IEC is likewise a global organization; however it concentrates on standards for electronics, electrical, and related technologies. Basic similarity concerns are in animal tracking (ISO-11784 and ISO-11785) and contactless proximity cards (ISO-14443) applications. The 1990s saw the acceptance of RFID as an important enabler in supply chain management, which spurred a further series of standardization activities.

A milestone came in 1996 with the standardization of RFID as a data carrier by the Article Number Association (ANA) and European Article Numbering (EAN) groups. In 1999, EAN International, and the Uniform Code Council (UCC) of the United States, now both known as GS1, adopted a UHF frequency band for RFID and established the Auto-ID Center at the Massachusetts.

Only recently have advances in silicon technology made RFID tags cheap and reliable. Thus, the first decade of the 21st century sees the world moving toward the technology's widespread and large-scale adoption. A major landmark was the announcement by Wal-Mart Inc., in the USA, to authorize RFID for its suppliers in "the near future," at the Retail Systems Conference in June 2003 in Chicago. This was followed by the release of the first EPC global standard in January 2005. Till date more than 1000 Wal-Mart locations have already implemented EPC RFID standard. This organization was charged with developing a global RFID standard for product labeling called the Electronic Product Code (EPC). The Auto-ID Center later evolved into Auto-ID Labs and EPC global Inc. The latter is a nonprofit organization, set up by UCC and EAN International, pursuing the commercialization of EPC technology.

3.4 Types of Tags in RFID

RFID tags fall into two categories, active tags, which contain an internal power source, and passive tags, which obtain power from the signal of an external reader. Because of their lower price and smaller size, passive tags are more commonly used then active tags for retail purposes. A passive tag consists of a microchip surrounded by a printed antenna and some form of encapsulation, plastic laminates with adhesive that can be attached to a product or a small glass vial for implantation. The tag reader powers and communicates with passive tags. The tag's antenna conducts the process of energy capture and ID transfer. A tag's chip typically holds data to identify an individual product, the product model and manufacturer. The difference between active and passive tags of RFID is given below in a table:

Table 1. RFID Active tag vs. Passive tag.

Active Tags	Passive Tags
Transmit a stronger Signal	Transmit a weaker Signal
Have a longer "read" range, can exceed 100 meters, Depending on antenna size	Read distance ranges of 10 cm. to a few meters
Operate at higher frequencies-commonly 455 MHz, 2.45 GHz, or 5.8 GHz	Typical operating frequencies- 128 KHz, 13.6 MHz, 915 MHz, or 2.45 GHz
Expire after battery power runs out	Operate until damaged or discarded
Cost a few dollars per tag	Cost 7.9 cents per tag when purchased in quantities of 1 million (as of May 2006)
Size is typically slightly larger than a deck of playing cards	Can be as small as a grain of rice

Without a power supply of their own, passive RFID tags depend upon the electromagnetic field of the reader. The paired power is improved and the electromagnetism is amplified to power up interior circuits. A multi-stage Greinacher half-wave magnetism or a derivative is normally used for this purpose. There are two different coupling techniques, near and far fields, which are used by passive tags.

3.4.1 Near Field Coupling

The EM field in the near-field area is sensitive in nature-the electric and the magnetic fields are rectangular and virtual-static. It mostly depends upon the type of antenna; one field (such as the electric field for a dipole or magnetic field for a coil) controls the other field. Most near-field tags rely on the magnetic field through inductive coupling to the coil in the tag. This mechanism is generally based upon Faraday's principle of magnetic induction. A current flowing through the coil of a reader

produces a magnetic field around it. This field causes a tag's coil in the vicinity to generate a small current. Communication between a reader and a tag is through a mechanism called load modulation. Any variation of the current in a tag's coil causes a small current variation in a reader's coil due to the mutual inductance between the two, and the variation is detected by reader. A tag varies the current by changing the load on its antenna coil, and hence the mechanism is called load modulation. Because of its simplicity, inductive coupling was initially adopted for passive RFID systems. Depending upon the application, near-field tags come in many form factors as shown in figure 3

The boundary between near-field and far-field regions is inversely proportional to frequency and approximately equal to c/2f, where c is the speed of light [3]. Therefore, only low carrier frequencies are used in near-field coupling tags; the two most common are 128 kHz (LF) and 13.56 MHz (HF). For example, the boundary distances are 372 m1 for 128 kHz and 3.5 m for 13.56 MHz One problem with use of low frequencies is that a large antenna coil is required. Also, the power of magnetic field of a magnetic dipole loop drops as 1/r6 in the near-field region, where r is the distance between a reader and a tag. Another downside is the low bandwidth and, hence, the low data rate

3.4.2 Far-Field Coupling

The EM field in the far-field region is radioactive in nature. Coupling here captures EM energy at a tag's antenna as a potential difference. Part of the energy incident on a tag's antenna is reflected back due to an impedance mismatch between the antenna and the load circuit. Changing the mismatch or loading on the antenna can vary the amount of reflected energy, a technique called backscattering.

Far-field coupling is commonly employed for long-range (5–20 m) RFID, and, in contrast to near-field, there is no restriction on the field boundary for far-field RFID. The Several emerging technologies in the UHF and LF bands try to exploit advantages of both near-field and far-field tags. UHF proponents are promoting near-field UHF tags for label tagging, which has been the sole domain of HF near-field tags. The advantage of using UHF here is the low tag cost, resulting from small antenna size. RuBee, a relatively new active RFID technology, operates in the LF band and employs long-wave magnetic signaling. It can achieve a read range of 30 m. Long-wave magnetic signaling has a great advantage: it is highly resistant to performance degradation near metal objects and water, a serious problem for UHF and Microwave far-field RFID.

RFID NFC anti-metal tag on mobile phone

Table 2. RFID/NFC anti-metal tag on smart phones

Antenna Dimension	**76X45mm (±0.2 mm)**
Final dimension	85X54mm (±0.5mm)
Antenna skip distance	88.6±0.4 mm
Antenna margin	7.0±1.0 mm
Width of the Tape	59.0±1.0 mm
Antenna number /square meter of typesetting	176 pcs

Table 3. RFID product features

Features of RFID (NFC, FFC) showing the various attributes with their standards and characteristic's:

Substrate Material	**Polyester Film （PET）**
The Antenna Material	Aluminum Etching
Surface Material	Wave-absorbing Material +Surface Label Printing
Characteristics	the Flexible Label
Product Attribute used in the metal surface	Waterproof, acid proof, alkali proof, collision and can be used outdoors, can be well effectively prevent metal of the radio frequency signal interference
Operating Frequency	13.0MHZ ～14.5MHZ
Supported Protocol	ISO/IEC14443-A
Chip IC	FM11RF08 (other compatible chips option)
MEMORY & SECURITY	1024bit X 8
Operating Mode	Inventory Read or Write
Reading Distance	≥1CM （Reader：Desktop Reader IVF-RH11）
Programming Cycle	100,000 cycles

Environmental Parameter of RFID

Table 4. Environmental Parameters.

Operating Temperature	-25℃～75℃
Storage Temperature	0℃～25℃

Table 5. Packing in RFID.

Packing in RFID

Core Diameter	76.2mm (3inch)
Volume Number	2000～5000PCS (According to Actual Demand)
The Roll Direction	the Surface or Printing Facing out (up)
Packing Material	Antistatic PE + Bubble Pad + Antistatic Bag + Paper Carton/Box

3.5 RFID Deployment and Concerns

Since RFID was first introduced in World War II to identify aircraft, the technology has improved as it has been implemented in a broad variety of uses, including identifying livestock and pets; shipping containers; managing vehicle fleets; increasing highway throughput; speeding up transactions at the point of sale; gaining entrance to buildings; real time asset tracking and mass transit ticketing. In the wake of 9/11, RFID is efficiently being utilized to boost the reliability of separate designs of recognition, without producing longer ID reliability verification wait times. Many collections of RFID exist in our daily life. Each requires to be verified separately. The technical and economic conclusions between the different collections explain that decisions in respect to the choice of users, including solution providers and other system integrators, hold the key to successful implementation of the future technology.

RFID is not yet a plug-and-play product technology. A few workers will take the "one-solution-fits-all" terminology, which leads to various difficulties and obstacles. Although, when the best design is preferred, it may require a self-design particular application to attain the excellent performance. The

settlements mostly require to be classified. For example, can the outstanding performance of a more costly self-design dominate the economics of employing an off-the-shelf design?

RFID under performs in some particular applications because of a non-optimized solution technique. The typical understanding of RFID, its collections, and self-design tools are important when calculating its future utilization in an auto ID program. Too often, the underlying engineering and physics are not understood, minimal training is provided, and expectations are unrealistic. Consumer privacy and data security concerns are heightened by the longer read distances capable with RFID. The technology creates an opportunity for unsolicited RFID tag data modifications (reads/writes), and/or reads of which the tag carrier is unaware. This concern is somehow unique to RFID forms of auto ID. Some collections of RFID have built-in security protocols to ensure only authorized readers talk with only authentic tags. Most of these secure collections also have technology design standards that limit data transaction distances to fingerbreadth, vs. feet, that takes care of data to reduce the threat from hackers. Another visible feature of security is whether to transfer particular ID data on the tag (and authorize data security to the reader framework), or having a specific RFID tag containing a "license plate" that connects to the real data, adhered in a secure master data base. This conclusion is mostly built on one application in a particular time. Measures and governances for RFID technology rest with the industry to which the wireless technology is being enforced.

With a limited inspiration, sustained by sci-fi computation, and the scarcity of brutal study, another concern hides. Someone who adopts the emergency of RFID-tagged commodities do that with practical clerical intensity. The concern of privately or secretly being tracked is perfectly impractical, but security issues are expanding as RFID is being employed in more private id applications, like passports, credit cards and retail goods tagging.

Another concern is the security of proprietary data. How much does one company want to reveal to a competitor to gain efficiencies? That dilemma is of special concern in extremely aggressive industries and companies, for example, pharmaceuticals. Sharing data in an open supply chain means the manufacturer may have to share its pricing throughout the supply chain, including its competitors. Databases supporting open supply chain networks must be built with the understanding that some data must remain protected.

The ultimate issue is the loss of global RF management regarding reader power, acceptable frequencies, and sideband spectrums levels. Likely, we know that our frugality is global, still there is a scarcity of typical settlements, and more efficiently the connected system achievement generates extra-ordinary changes, engineering expense-effective solutions for the Universal open supply series is challenging and complicated. This scarcity of Universal standardization and regulation prevents the approval of RFID as an open supply series mechanism.

The terminology explains that RFID technology has the power to impact the supply series, both positively and negatively. The potential to transfer information digitally, during the entire life of services and goods, will generate an enormous transformation in the global supply series operations and helps in providing authentic goods reach their destination. That a product can bisect the whole shipping and distribution network easily does not imply that the means to manage it will be simple. This is first phase of utilizing the technology globally.

3.6 Frequency Bands in RFID

RFID tags are divided into three regions with respect to frequency:

- Low frequency (30 - 500kHz, LF)
- High frequency (10 - 15MHz,HF)
- Ultra high frequency (5.8GHz, 2.4 - 2.5GHz, 850 – 950MHz, , UHF)

Low frequency tags are inexpensive than any of the powerful frequency tags. These are secure and quick sufficient for some of the particular applications, although there is massive quantity of data available, a tag has to stay in a reader's spectrum and it will boost the duration. Another benefit is that low frequency tags are slight damaged by the existence of fluids or metal. The disadvantage of such type of tags is their limited reading spectrum. The most particular frequencies used for low frequency tags are 140 - 148.5 kHz and 125 - 134.2 kHz. Long frequency tags have higher transmission rates and ranges but also cost more than LF tags. Smart tags are the most global member of this group and they work at the frequency spectrum of 13.56MHz.

In comparison to various tags, UHF tags have the highest spectrum of all tags. The spectrum ranges from 3-6 meters for passive tags and 30+ meters for active tags. Apart from that the transmission rate of UHF tags is also very high, which permits to read a single tag in a real manner of time. This attribute is very crucial where tagged entities are moving with a high speed and remain only for a short time in a readers range. Also, UHF tags are more expensive than the native tags and are generally affected by fluids and metal. So, with the help of these excellent properties this is main reason that UHF tags are particularly useful in automated toll collection systems. Typical Frequencies are 950MHz (Japan), 868MHz (Europe), 915MHz (USA), and 2.45GHz. Frequencies for LF and HF tags are license exempt and can be utilized globally; however frequencies for UHF tags differ from Nation to Nation and needs the permission for communication.

3.7 Working of RFID

RFID is virtually the information which is transported by the radio waves. The future technology came into existence from the fields of radar and radio engineering. Magnetic or electromagnetic fields have been used for the data transfer between the RFID transponder and the reader and, in passive RFID collections, are also used to hand over the power supply to the RFID transponder.

The components of an RFID field are:

The transponder or "tag" is the data transporting component of an RFID system. RFID tag data space normally ranges from a few bits to several kilobytes. A tag generally having an electronic microchip and chip antennae designed to permit communications with a reader. In a "passive" system the tag is mechanized by pairing with the reader field. An active tag may be totally or partially mechanized through its own battery source. Tags may be designed to be read-only or to read and accept writes. Tags are typically clustered for the clear-cut application. Tags may be planted in a collection of materials, including plastic cards, paper cards, injection molded plastics (such as key fobs), and glass (for use in a bodies such as animal identification). The typical method used for sending data from the transponder back to the tag is backscatter, in which the frequency of the reflected wave correlates with the frequency of the transmission from the reader. The transponder, or 'tag', consists of:

1. A microchip. These are now in our day life as small as 0.4mm by 0.4mm. Size of the microchip is often a principal factor in its cost, since the smaller the chip, the greater the produce from a constructed cracker. The cracker is processed by being manipulated to final chip consistency, speculated into separate chips, and further more knocked for fasten, wire, or flip chip connection to

an antenna. The chips are basically factory-programmed with an ID number during their contact testing stage. This pre-programming allows the utilization of the separate chip number in later stages of testing.

2. A chip antenna, designed for either electromagnetic or magnetic fields. The antenna is originated on a typical substrate (e.g., PET). The antenna can be etched copper, wires, etched aluminum, or printed conductive silver ink, and a growing array of aluminum or copper antennae are being made with preservative processes, such as electroplating. The material of antenna does edict positive achievement characteristics, and a particular type may be more optimal in a given application. Wire antennae are often used in 125-134 kHz (lf) tags, as the high number of winding turns required at this frequency is easiest to achieve in a realistic footprint with small diameter wires.

The connection operation is used to secure the chip onto the antennae substrate and electrically connect the chip to the antennae. The chip bumping technique, antennae information, and connection operation must be engineered together. After chip connection, decorate is RFID-functional and is ready to be packaged. Once decorate is packaged into a label, paper ticket, plastic card, or other material, a final test is typically conducted on each unit, and non-conforming units are highlighted and sometimes completely removed. The testing also permits writing to be done to each chip with respect of a rare ID number. Programming of large data or object specific data, such as an electronic product code (EPC), is normally done near the end application (for example, with an RFID-enabled bar code printer systems). The reader typically consists of a radio frequency receiver and sometimes a transmitter, a control unit, and antennae to provide data retrieval or communication: It can be thought of as a digital communications system. The chips and reader can be arranged to be Read-Only or vice-versa. Also readers may also be arranged for the communication with the capability to transmit the received data to another destination (e.g., via RS 232). The reader is used to provide commands to the tag, timing pulses and data, as well as paired energy for passive tags. It also receives data from the tag and must decipher this data relative to ambient RF noise. Most readers are designed to operate at a single channel or frequency. There are some designs that can read multiple protocols at different frequencies, but single channel frequency readers rule the day.

Reader system sizes range from the large fixed reader systems (size similar to shoplifting gates used in retail stores and libraries) that have the highest energy (and thus the longest read distances), to the smaller mid powered readers, and even smaller handheld readers powered by batteries. A unique feature of RFID is the ability to have multiple tags in the read field simultaneously. The system design feature that allows this is referred to as anti-collision. Anti-collision protocols are now part of many RFID standards, so that any vendor's chip can work with any vendor's reader when both are designed per a common set of standards. Anti-collision performance varies from reading a few tags per second to hundreds per second, depending on the frequency, the standard, and the amount of data on the chip to be read.

The reader antenna is important to the RF operation of the reader. Reader antennae designs can be made to maximize read distance, requiring tighter tolerances for the tag-to-reader coupling orientation, or they can be designed to be more robust to the tag-to-reader coupling orientation, but sacrifice some read distance.

The Federal Communications Commission (FCC) regulates the frequency and reader system RF emissions. RFID is operated at a shared frequency band, so care must be taken to prevent cross

interference of RF systems sharing the same frequency band. Software for RFID-derived data is typically designed to filter the large amounts of repetitive data capture inherent in many RFID systems. This filtered data is then used by application-specific host systems. Higher end readers may have data filtering capability designed in. The software may also act as a data verifier and require multiple tag reads at a given reader before accepting that tag as a legitimate. Table 6. Explaining a comparison study of various types of operational frequencies of RFID with respect to NFC and FFC.

Table 6. Summary of Operational Frequencies.

Frequency Ranges	**LF 125 KHz**	**HF 13.56 MHz**	**UHF 868-915MHz**	**Microwave 2.45 GHz & 5.8 GHz**
Typical Max Read Range (Passive Tags)	Shortest 1”12”	Short 2”24”	Medium 1’-10’	Longest 1’15’
Data Rate	Slower	Moderate	Fast	Faster
Applications	Access Control & Security Identifying widgets Through manufacturing processes or in harsh environments Ranch animal identification Employee IDs	Library books Laundry identification Access Control Employee IDs	Supply chain tracking Highway toll Tags	Highway toll Tags Identification of private vehicle fleets in/out of a yard or facility Asset tracking
Tag Power Source	Generally passive tags only, using inductive coupling	Generally passive tags only, using inductive or capacitive coupling	Active tags with integral battery or passive tags using capacitive storage, Efield coupling	Active tags with integral battery or passive tags using capacitive storage, Efield coupling
Ability to read Near metal or wet surfaces	Better	Moderate	Poor	Worse

3.8 Proposed Structure and Design of RFID System

As shown in the Figure4, the process begins when RFID tag comes in the range of the RFID reader then the reader transmits the signals to the tag. Then tag will modulate that carrier signal with the data present in it. Then this modulated signal will be received by the RFID reader.

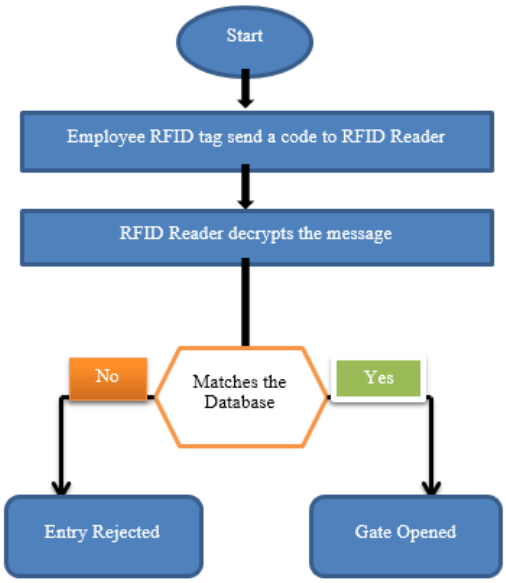


Figure. 4. Flow Chart Design of RFID based Security System.

The reader is having the RS232 interface so the data will be transferred from the transmitter (Tx) pin of reader to the 3rd pin i.e. transmitted data (TxD) pin of the RS232 port. Then the data is taken from TxD pin and is given to the 13th pin of the MAX 232 and output is taken from the 12th pin of MAX232 and is given as the input for the microcontroller. Here MAX232 will change standards from RS232 level to the TTL level standards. The input is given to the Rxd (P3^0) pin of 8051 microcontroller. In the microcontroller there will be code for the identification of the person and output which is either low (0) or high.

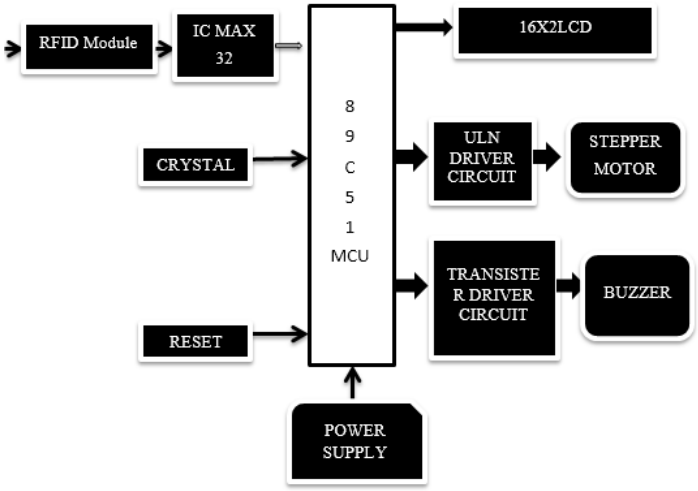


Figure. 5. Architecture of RFID Security System.

The output is taken from the additional port pins. The micro controller will analyze the input data of tag with stored data of the certified person and ports the output pin either to low or high. The data from the receiver module is sent to the relay which stands as the switch to the load. Relay is an electromechanical device. When the 5v signal is given to the circuit then magnetic energy will be produced and this magnetic energy will drive the switch from the NC point to the NO and a current passes through the motor and letting it to work to open a door.

3.9 RFID advantages

RFID advantages are given below:

- Reader can read and write data to RFID tags without any direct communication and no line of complication problem.
- Data from the different RFID tags are accessed by the reader by radio waves.
- No maintenance costs; RFID can work under different atmospheres and can be utilized efficiently for over 10 years.
- Fast read and write with the duration taken for read/write being a few milliseconds.
- Future generation RFID tags are made with excellent memory capabilities ranging from 16 - 64 Kbytes which is highly efficient than a typical barcode.
- RFID tags can work with GPRS and has been used for tracking.
- RFID tags can also integrate with other technologies. For example, it is used with wireless sensor net-works for better connectivity.

3.10 RFID Security

The principal and ultimate security issue of RFID technology is that anyone can access the RFID data because there is no line of sight complication that will be capable to gather data. Apart from that, people are copying RFID tags and using them just as the way it was done for credit cards before. Protecting effective copying of RFID tags are still an open and challenging issue for the next generation network infrastructures. Criminals with RFID readers could scan clusters for efficient value of bank notes. Also terrorists could scan digital passports to target particular nationalities.

Currently the research is on-going on RFID malware. RFID technology malware can be categorized into three different categories:

- Exploits,
- Worms, and
- Viruses.

RFID exploits are conventional hacking attacks that are identical to those found on the Internet like buffer overflows, code insertion, and SQL injection attacks. RFID worms and viruses are generally RFID exploits that copy the original exploit code to newly appearing RFID tags. The main difference between these two is that RFID worms trust on network connections whereas RFID viruses do not.

4 Near Field Communication vs. Far Field Communication for the Future Generation Network Infrastructures

Near Field Communication and Far field Communication both fall in the category of Radio Frequency Identification. In this part of study we are trying to differentiate the implementation issues of NFC and FFC on this basis of Radio Frequency Identification.

Near-field communication: The antennas of RFID reader transmit electromagnetic radiation or what we can say radio waves. So, if the RFID tag is in the range of the space complete wavelength of the reader, then under some conditions it is spoken to be in the "near field" (as with various RFID terms, illustrations are not properly identified). If in case, RFID tag is more than the distance of one complete wavelength across, then it is said to be in the "far field." The signal of the near field wireless communication technology blights as the cube of distance from the antenna, while as, signal of the far field wireless communication technology blights as the square of the distance from the antenna. Accordingly, passive RFID systems that commit on near-field communication (Normally L and HF

systems) have a lesser read range in comparison to those that utilize far field communication (UHF and microwave systems).

Far Field Communication -- In Far Field Communication an interrogator antenna the tag are connected under one full wavelength of the carrier wave. The far field signal blights as the square of distance from the antenna, and is generally utilized in Ultra High Frequency and Microwave systems. Far Field Communication manipulates a backscatter radio link [http://rfidsoup.pbwiki.com/Far+Field+Communication]. RFID reader antennas transmit electromagnetic radiation (radio waves). Accordingly, when the RFID tag is outside of one full wavelength of the reader, it is called to be in the "far field." If it is within one full wavelength away, it is called to be in the "near field." The far field blights as the square of the distance from the antenna, when the near field signal blights as the cube of distance from the antenna. Thus, passive RFID systems that commit on far field communications (particularly UHF and microwave systems) have a greater read range than those that utilize near field communications (normally low- and high-frequency systems).

Finally, we will provide the comparison survey of both these applications for the next generation network infrastructures to fulfill the aim of the methodology and implement the socio- technical undercurrent's for the future generation network standards.

Table 7. Comparison of NFC vs. FFC on the basis of Technology.

S. NO.	Attributes	NFC (HF)	FFC (UHF)	Remarks
1	Collision	Rare	Rare, Avoided by	No collision of reading tags and readers in NFC. In FFC, It is avoided through standardized algorithms approved by GS1 and GS2
2	Form factors of Design	Standardized	Customizable	UHF can be tamper proof windshield tags to avoid theft or misuse
3	Communication Protocols	Standardized	Proprietary and open	Development effort is more in UHF
4	Data Transfer Speed	Low	Fast	Faster speed gives faster processing in UHF
6	Environmental Factors	Resistant to water/metal	Read range affected by water/metal	UHF has effects on read range due to interference by metallic or liquid platform unlike HF due to working principle difference
7	Working Principle	EM Field interaction	Backscattering of EM waves	Field interaction can happen in closure distances only (NFC) no EM emission in HF unlike UHF
8	Security/Authentication	Data stored in tag itself	Information stored and server authentication required	NFC is more Vulnerable for data theft
9	Range Control	Up to 1 Meter	Up to 12 meters	Better Range, Better Visibility, Better Operations
10	Ambient Factors (Temperature, Humidity, Ruggedness)	Taken care by manufacturer following CE and GS standards	Taken Care by manufacturer following CE and GS standards	Similar in both HF and UHF. IP 42 AND IP 65 protection

Table above showing comparison on the basis of Technology, further more now we are showing the comparison on the basis of Operations and Management of NFC and FFC for the Next Generation Network Infrastructures.

Table 8. Showing Comparison on the basis of Operations and Management

S. NO.	Attributes	NFC (HF)	FFC (UHF)	Remarks
1	Waiting Time	More	Less	Due to read range and faster data transfer, UHF has its advantages over HF based systems
2	Design	Standardized	Tamper Proof	UHF tags cannot be removed, misused or stolen
3	Security	All information stored in card only	Only unique ID and basic data Stored in tags, server verification also required	2 levels of verification process makes UHF more safer
4	Boom Barrier Operation	Complete cycle for each pass	No need to complete a full cycle for each pass. Auto response through loop detectors or anti-crash sensors	Life of boom barrier and energy saving is more in FFC in comparison to NFC
5	Ease-of-use for users	Stop, roll down window, go near the reader	Automatic Reading from distance	A user needs to stop at closure distance to reach the reader or step down from the car to authenticate in NFC, No such hassles in FFC
6	Queue management	One by one reading form close proximity, no multiple reading capabilities	Automated reading from controlled distance and Multiple reading capabilities	Queue Management becomes faster in FFC due to automated reading and multiple reading capabilities
7	Future Prospects	1) Cannot be integrated and used in large and high transition parking guidance or Asset mgt (No RTLS) or Guard patrolling systems 2) Not suited for locating parked cars in busy and large parking	1) Can be integrating and used in large and high transition parking guidance system or Asset Tracking systems or Guard Patrolling systems (on demand –Auto RTLS) 2) Can be utilized for locating your parked car	1) Auto parking guidance system during peak hours requires a high speed and long range technology to avoid conjunction i.e., FFC based systems 2) Future Integration for other desired solution can be possible with Long Range Technologies only i.e. on demand-Automated Real Time Asset Tracking or guard patrolling systems 3) Location search for parked car for future

Comparison between two wireless technologies (NFC vs. FFC) with respect to Economics and Management.

Table 9. Comparison of NFC VS. FFC on basis of Economics and Environment.

S. NO.	Attributes	NFC (HF)	FFC(UHF)	Remarks
1	Cost Of Technology	Readers are of same price, cards are costlier	Cheaper tags/cards	1) Readers of both HF and UHF come at almost same price but UHF tags are cheaper than HF cards 2) Price factor is necessary to consider for consumables as it is needed continuously
2	Green Concept	More Co2 and Co emission during entry-exit and parking slot search, leading to more cost to control and maintain air ambience	Lesser waiting time leads to lessor CO2 and CO emissions	FFC based solution should be preferred for Advent's "Green Technology Philosophy"
3	Service and Support	Readily Available	Readily Available	Hardware components, spare parts, servicing options etc. are readily available for both the technologies
4	Cost of Operation	Slightly Cheaper	Slightly Cheaper	UHF is slightly higher due to slightly higher energy consumption as it works on backscatter principle unlike HF
5	Fuel Consumption	More fuel consumption due more waiting time	Better fuel management benefits during entry-exit of cars and automatic parking guidance in parking lots	FFC certainly has advantages over NFC in Fuel ROI
6	Cost of maintenance	Cheaper	Moderate	Maintenance of UHF based systems are relatively higher than HF

5 CHALLENGES AND DISCUSSION

RFID technology faces numerous implementation challenges. The major challenges include technological capability, Universal regularity, government rule and regulations, and cost as summarized in Table 10 and described below:

Table 10. RFID implementation Challenges

Levels	Challenges
Fundamental	• High Capital costs • Challenges in finding the ROI • Challenges in finding the "drivers" for adoption.
Technical	• Imperfect read-rates • Unproven systems • Difficulties with capturing low-cost tags • Uncertainty about the role of the middleware • Lack of in-house experts to implement RFID
Security	• Issues regarding the compromise of data during wireless transmission • Uncertainty around security of data storage and physical security of storage site
Privacy Issues/ Govt. Regulations	• Privacy issues and the potential for legislation • Uncertainty around Standards

At present, the NFC technology has reached a level where commercial launch preparation can begin and should be established. However, to some extent definite standards for NFC services are still missing:

- The scarcity of an ultimate conclusive approach for the development of NFC services originates in a vital conflict between several involved key actors including mobile phone manufactures, network operators, banks and other service providers: every party indeed tries to enforce its interests and wants to play a major role in the flow of the application scenario and the associating acquisition of big money.
- Third-party income producers, cognate banks and different financial associations, need to anchor NFC applications in unbiased space on the mobile phones, while network operators of course want to charge clients for presenting services hosted in protected atmosphere on the UICC. Due to different workloads in NFC applications, they are also busy in custody of the highlighted wireless network infrastructures and can thus control any SMS-based remote over-the-air authority potentials that might be utilized to efficiently design or modernize NFC services on the handset.
- The mobile phone manufacturers on the other hand decide which sort of NFC hardware and which alternative forms of dedicated Secure Element chips are actually implemented in the handset. And on higher layers, of course also the phone's operating system needs to provide appropriate NFC support.
- Google already offers mature NFC interfaces for developers within their own Android operating system and - in partnership with several banks and the assistance of a handset manufacturer – managed to publish a fist qualified application for mobile NFC payment. Competitors from Apple and Microsoft indeed also announced plans to develop smartphones with NFC backing in the next generation, but the
- Thing is that, it is still uncertain how exactly their concept will look like. Nevertheless, this means that NFC applications are still handset specific.
- A simple, dynamic and platform-independent framework is missing and difficult to realize. In a certain way though, a collaboration of stakeholder, in particular phone manufacturers and network operators, is definitely needed for developing sophisticated and usable NFC services for the mass market.
- Mobilization and authenticity of NFC applications are perhaps the ultimate determinants of the user understanding in day to day use of the NFC technology and accordingly crucial keys to its prosperity.

6 Conclusion

RFID is still in an emerging stage and furthermore is in the pipeline in terms of up to date applications, Various Researches can be done through this technology. Between applications which have been developed earlier, RFID tags are being utilized in dressing for invoice and security issues. RFID tags are embedded inside animals for tracking concerns. RFID tags placed in dresses can be used to be aware about the number of hours an employee spends to complete a particular its work. There are numerous organizations that are pro-testing against the use of RFID to track people fearing the impact on people's social life and privacy. Clearly the extent to which use RFID is to be used is still an open debate. A large type of articles on RFID tags are ongoing including on embedding these with different devices, particularly on mobile devices. RFID users and makers are looking for complete standardization and requirement of RFID. As the cost of applications sink too and technological enhancements continue to exist, RFID technology is supposed to grow economically and technically more feasible and influence our daily lives when more applications are being developed. RFID technology authorize users to enhance perfection, presents superior data flow management, higher data processing speeds, amplified security and minimization of bugs through authentication and automation. It further helps concluding cost savings and ROI from both implementer and user standpoint. In order to conclude these enhancements, it is important that an RFID Professional knows and understand the distinct differences between HF and UHF RFID to execute the accurate abilities and fluctuations to assemble the particular application requirements.

Near Field communication technology allows its users to conceptualize and undergo a brand new and inspiring universe. It has facilitated its users with a variety of applications. However, there outlets two faces of coin, NFC technology also got affected from one such coin as well. It follows various particular threats that don't allow users to take a good use of it. This study describes different applications scenarios of RFID, NFC and FFC, and outlines series of threats and its respective counter measures to protect these short-range wireless technologies. These deportments can be used to provide security to applications using NFC technology and also attract more users to use it without any problem statement. Further, the paper would be very helpful for new learners to understand RFID, NFC, FFC Next Generation wireless technologies, its applications, threats and security constructs used for protecting it. It also animates researchers to launch some global assistance for securing these wireless technologies from threats to build user's confidence in technology to use it further for the Future Generation Wireless Network Infrastructures.

ACKNOWLEDGEMENT

We are thankful to all the Faculty members of Computer Science and Engineering Department, Shri Ramswaroop Memorial University Lucknow Uttar Pradesh for their motivation and continuous support. Our special vote of thanks to Dr. Bineet Gupta for their valuable suggestions and contributions.

REFERENCES

[1] Sanjay Ahuja, Pavan Potti "An Introduction to RFID Technology", School of Computing, University of North Florida, Jacksonville, Florida Communications and Network, 2010.

[2] Simon Burkard "Near Field Communication in Smartphones", Master Student, Computer Engineering Dep. of Telecommunication Systems, Service-centric Networking, Berlin Institute of Technology, Germany.

[3] Chetna Bajaj, "Near Field Communication", International Journal of Advanced Research in Computer Science and Software Engineering, Department of Computer Science & Engineering, Ambedkar Institute of Advanced Communication Technologies and Research, Delhi, India, Volume 4, Issue 8, August 2014.

[4] IEEE USA "The State of RFID Implementation and Its Policy Implications: An IEEE-USA White Paper", 15 April 2009.

[5] Vipul Chawla and Dong Sam Ha, "An Overview of Passive RFID", Virginia Polytechnic Institute and State University, IEEE Applications & Practice, September 2007.

[6] Vibhor Sharma, Preeti Gussian, Prashant Kumar "Near Field Communication", Department of Computer Science & Engineering Tula's Institute, The Engineering and Management College, Dehradun, Uttarakhand 248001, India, Conference on Advances in Communication and Control Systems 2013 (CAC2S 2013).

[7] Arun N. Nambiar "RFID Technology: A Review of its Applications", Proceedings of the World Congress on Engineering and Computer Science, San Francisco, USA. 2009 Vol II WCECS 2009, October 20-22, 2009,

[8] K.Srinivasa Ravi, G.H.Varun, T.Vamsi, P.Pratyusha "RFID Based Security System", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-5, April 2013.

[9] Mohsen Attaran, "Critical Success Factors and Challenges of Implementing RFID in Supply Chain Management", California State University, Bakersfield, CA, USA. Journal of Supply Chain and Operations Management, Volume 10, Number 1, February 2012.

[10] Xiaozheng Lai, Zeming Xie, and Xuanliang Cen, "Compact Loop Antenna for Near-Field and Far-Field UHF RFID Applications", School of Computer Science & Engineering, South China University of Technology, Guangzhou 510006, China, Progress In Electromagnetics Research C,Vol-37, 171-182, 2013.

[11] Yuan Yao, Junsheng Yu, and Xiaodong Chen, "Study on the Optically Transparent Near-Field and Far-Field RFID Reader Antenna", Beijing Key Laboratory of Work Safety Intelligent Monitoring, School of Electronic Engineering, Beijing University of Posts and Telecommunications, No. 10 Xitucheng Road, Beijing, China, Hindawi Publishing Corporation International Journal of Antennas and Propagation, Article ID 149051, Volume 2014.

[12] M. MABROUK , M. DHAOUADI, T.P. VUONG , A.C DE SOUZA, A. GHAZEL, "A Broadband UHF TAG Antenna For Near-Field and Far-Field RFID Communications", Laboratoire GRESCOM, SUPCOM de Tunis, University de Carthage, RADIOENGINEERING, VOL. 23, NO.4, DECEMBER 2014 – ERRATA.

[13] Jignesh Patel, Badal Kothari, "Near Field Communication - The Future Technology For An Interactive World", Int. J. Engg. Res. & Sci. & Tech. 2013 ISSN 2319-5991 Vol. 2, No. 2, May 2013.

[14] Gowher Mushtaq, Shashank Singh, Neeraj Kumar Tiwari, "To Study the Energy Efficient Deportments of Existing Attributes for Next Generation Network Infrastructures", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-4 Issue-4, April 2015.

[15] Mohammad Umair Yaqub, Umair Ahmad Shaikh, "Near Field Communication -Its Applications and Implementation in K.S.A.", King Fahd University of Petroleum & Minerals, 13th of February 2013.

[16] Asawari Dudwadkar, Akhil Gore, Tushar Nachnani, Harshil Sabhnani, "Near Field Communication in Mobile Phones", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-3, Issue-1, October 2013.

[17] Tomasz Dlugosz, Hubert Trzaska, "How to Measure in the Near Field and in the Far Field", Wroclaw University of Technology Institute of Telecommunications, Teleinformatics and Acoustics, Wyspianskiego, Wroclaw, Poland, Communication and Network, 2, 65-68, 2010.

[18] Coskun, V., Ozdenizci, B., & Ok, K, "A Survey on Near Field Communication (NFC) Technology". Wireless personal communications, 71(3), 2259-2294, 2013.

[19] Ari Juels, "RFID Security and Privacy: A Research Survey", IEEE Journal on Selected Areas in Communications, VOL. 24, NO. 2, February 2006.

TNC Transactions on Networks and Communications
SOCIETY FOR SCIENCE AND EDUCATION UNITED KINGDOM
VOLUME 3, ISSUE 3
ISSN: 2054 - 7420

An Amalgamated Approach of Fuzzy Logic and Genetic Algorithm forBetter Recruitment Process

[1]Anju Khandelwal and [2]Ashish Agrawal
[1]Uttar Pradesh Technical University, India;
[2]Shri Ram MurtiSmarak College of Engineering & Technology, Bareilly
dranjukhandelwal@rediffmail.com, agarwal.ashish01@gmail.com

ABSTRACT

The recruitment process in any departments or organizationsis usually decided by traditional criteria. In today's scenario, every organization wants to have best employees for their work. Many organizations are used to have separate departments to solve this purpose. But sometimes the recruitment process gets affected by human perceptions, beliefs, pat experiences, feelings, personal relations etc..So, for making recruitment process more automatic and accurate, various authors have proposed their solutions with Hungarian method. In this paper, authors are proposing a method of recruitment by the use of fuzzy triangular number and genetic algorithm with Hungarian method. After performing the first stage (written test) of recruitment with fuzzy triangular number and Hungarian method, the later stages are accomplished with linguistic variables and final recruitment is performed by the use of genetic algorithm.

Keywords: Fuzzy number, Triangular Fuzzy Number, Job Recruitment, Robust Ranking Method, Hungarian method, Linguistic Variable, Genetic Algorithms.

2000AMS Subject Classification: 90C08, 91B24, 91B18

1 Introduction

The assignment problem is a special type of Linear Programming Problem in which our objective is to assign n number of jobs to n number of persons at a minimum cost/ maximum profit. Assignment may be persons to jobs, classes to rooms, operators to machines, drivers to trucks, trucks to delivery routes, or problems to research teams, etc...Thesolution of assignment problem is defined by Kuhn[1] named as Hungarian method. To find solutions to assignment problem, various another algorithms such as Neural Network [2], Genetic Algorithm [3] etc. have been developed. Over the past 50 years many variations of the classical assignment problems are proposed e.g. Generalized Assignment Problem, Quadratic Assignment Problem, and Bottleneck Assignment Problem etc. However, much of the decision making in the real world takes place in an environment where the objectives, constraints or parameter are not precise. Therefore a decision is often made on the basis of vague information or uncertain data. In 1970, Belmann and Zadeh introduced the concept of fuzzy set theory into the decision making problems involving uncertainty and imprecision. Fuzzy Assignment Problems have received great attention in recent years. Lin and Wen [4] proposed an efficient algorithm based on the labeling method for solving the Linear Fractional Programming Problem. Chen[5] discussed a fuzzy assignment model that considers all persons to have same skills. Long-Sheng Huang and Li-puZhang[6] developed a mathematical model for the fuzzy assignment problem and transformed the model as certain assignment problem with restriction of qualification.

DOI: 10.14738/tnc.33.1080
Publication Date: 15th May 2015
URL: http://dx.doi.org/10.14738/tnc.33.1080

Linzhong Liu and XinGoa[7] considered the Genetic Algorithm for solving the fuzzy weighted equilibrium and multijob assignment problem.

GA (genetic algorithm) simulates the survival of the fittest individuals among all the individuals in the population over successive generations for solving a problem. Genes from good individuals propagate throughout the population so that two good parents will sometimes produce offspring that are better than either parent. Thus either successive generation will become more suited to their environment [16, 17].Jiuping Xu[8] developed a priority based Genetic Algorithm to a Fuzzy Vehicle Routing Assignment model with Connection Network. The total cost which includes preparing costs as the objective function and the preparing costs and the commodity flow demand is regarded as fuzzy variables. There are several papers [9-11] in the literature in which generalized fuzzy numbers are used for solving real life problems. Also Dominance of Fuzzy Numbers can be explained by many ranking methods [12-15].

2 Preliminaries

In this section, some basic definitions are discussed.

2.1 A Fuzzy Set is characterized by a membership function mapping element of a domain, space or the universe of discourse X to the unit interval [0,1] i.e. $A=\{(x,\mu_A(x);x\in X\}$. Here : $\mu_A : X \to [0,1]$ is a mapping called the degree of membership function of the fuzzy set A and $\mu_A(x)$ is called the membership value of $x\in X$ in the fuzzy set A. These membership grades are often represented by real numbers ranging from [0,1].

2.2 A Fuzzy Set $\tilde{A}$, defined on universal set of real number X, is said to be fuzzy number if,

i. $\tilde{A}$ is convex, i.e. ~ $\mu_A\square(\lambda x_1+(1-\lambda)x_2)\geq \min(\mu_A\square(x_2)), x_1, x_2\in X, \lambda\in[0,1];$

ii. $\tilde{A}$ is normalized fuzzy set if there exist at least one $x_0\in X$ with $\mu_A\square(x_0)=1$

iii. Its membership function $\mu_A\square(x)$ is piecewise continuous.

2.3 For a Triangular Fuzzy Number A(X), it can be represented by A(a,b,c;1) with membership function μ_x given by

$$\mu(x)=\begin{cases} l(x)=\dfrac{x-a}{b-a}, & a\leq x\leq b \\ 1, & x=b \\ r(x)=\dfrac{c-x}{c-b}, & b\leq x\leq c \\ 0, & \text{otherwise} \end{cases}$$

Where $\mu\square 1(x)$ and $\mu\square r(x)$ are the left membership function and right membership function of the fuzzy set.

2.4 A Triangular Fuzzy Number $A = (a,b,c;1)$ is said to be non-negative if and only if $a \geq 0$.

2.5 **α-Cut:** The α-Cut of a fuzzy number $A(x)$ is defined as $A(\alpha) = \{x / \mu(x) \geq \alpha, \alpha \in [0,1]$.

2.6 **Genetic Algorithm**:The basic idea behind the genetic algorithm is to manage and maintain a population of chromosomes (collection of genes) and to search for a solution until a nearest

optimum solution is found. GAs has got a great measure of success in search and optimization problems. Some major terms of Genetic algorithm are-

- Fitness Function-The fitness function used in this paper is –

$$\text{Fitness Function} = \left(\sum_{i=1}^{n} Chromosome's\ \text{Gene Value} - 1\right)$$

- Arithmetic Crossover-The basic formula for performing arithmetic crossover is-

Offspring 1: a*parent1+ (1-a)*parent2
Offspring 2: (1-a)*parent1+ (a)*parent2

- **Boundary Mutation-**For performing boundary mutation, the range is 0-26 and 26 was selected to replace the middle gene.

2.7 Fuzzy Assignment Problem

In everyday life corresponding to each physical structure there is some mathematical phenomena. Here we describe mathematical model of assignment problem in the fuzzy theory for delegation of post in recruitment process.

Assume that there are n jobs and n persons.The assignment cost influenced by different parameters in real life and therefore assignment cost coefficients are usually uncertain value and will change respectively in different time frames. In this paper we consider assignment cost as a fuzzy number and defined by $\tilde{c} = (\underline{c} / c / \overline{c})$ where c represent the most possible assignment cost, c the most optimistic assignment cost and c the most pessimistic assignment cost. Obviously if cost coefficients are fuzzy numbers, then the total assignment cost becomes fuzzy as well.Now, the fuzzy assignment problem is written as,

$$Min.\ \tilde{z} = \sum_{i=1}^{n}\sum_{j=1}^{n} \tilde{c}_{ij}\ x_{ij}$$

Subject to

$$\sum_{i=1}^{n} x_{ij} = 1,\ j = 1,2,3,\ldots\ldots\ldots\ldots,n$$

$$\sum_{j=1}^{n} x_{ij} = 1,\ i = 1,2,3,\ldots\ldots\ldots\ldots,n$$

$$x_{ij} \in \{0,1\} \text{ for } i, j = 1,2,\ldots\ldots\ldots\ldots,n$$

2.8 Robust's Ranking Method

In this paper we defined the fuzzy cost coefficient into crisp ones by a fuzzy number ranking method. For this we use Robust's ranking method which satisfies compensation, linearity, and additive property and provide results which are consistent with human intuition.

If $\overline{c}$ is a fuzzy number then the Robust's ranking is defined by

$$\tilde{R}(c) = \int_{0}^{1} 0.5(c_l, c_u)\, d\alpha$$

Where (c_l, c_u) is the alpha level cut of the fuzzy number.

3 Problem Statement

In every organization, employee hiring is a vital and huge task which sometimes becomes tough row o hoe. Suppose , in an organization A, hiring process is going on for four job designations- TM(Technical Manager), HRM(Human Resource Manager), FM(Financial Manager)and PDM(Post Development Manager). For the TM designation there are 2 vacancies, for HRM there are 4 vacancies, for FM there

are 3 vacancies and for PDM there is 1 vacancy. It means, they have to hire total 10 people. After calling for resume, total 50 candidates applied for this recruitment. Now the problem is to hire the most suitable candidate for the defined designations, and another main task is to make this process faster and more accurate.

4 Implementation

Out of total 50 candidates we made 5 groups containing 10 candidates in each

Section 1-

- Group 1-[C1 C2 C3 ……C10]
- Group 2-[C11C12C13…….C20]
- Group 3-[C21 C22C23…….C30]
- Group 4- [C31 C32 C33…….C40]
- Group 5-[C41 C42 C43…….C50]

At first stage,authors had conducted a written test, which had 25 marks questions forTM, 25 marks questions for HRM, 25 marks questions for FM, 25 marks questions for PDMs. The data in further tables (table 1- table 5) is calculated by performing the Robust Ranking method. As in table 1 for C1, the value in TM column is 12 which is calculated as, (it means C1 scores 12 marks in TM section).(Note:Scale Taken-[10-25] for marks)

Fuzzy Triangular Number-(10, 12, 14)

$$(C_k^l, C_k^u) = [2k+10, 14-2k]$$

$$= 24$$

$$R(\check{C}) = \int_0^1 0.5 * 24 dk$$

$$= \left[12k\right]_0^1$$

$$= 12$$

Then **at*second stage*,**after applying Hungarian method, we found 4 best candidates from each group. It means 20 candidates out of 50 were shortlisted.

Table 1: Candidates and their marks for group 1

Candidates / Designations	TM	HRM	FM	PDM
C1	12	18	20	15
C2	16	19	14	20
C3	22	24	15	15
C4	14	22	19	13
C5	16	18	24	21
C6	18	15	25	20
C7	16	17	12	21
C8	18	19	22	23
C9	24	11	16	15
C10	15	18	21	10

Table 2: Candidates and their marks for group 2

Candidates / Designations	TM	HRM	FM	PDM
C11	16	20	25	21
C12	15	22	19	16
C13	14	24	18	14
C14	22	16	20	25
C15	23	19	21	15
C16	13	20	24	21
C17	10	15	19	17
C18	14	23	16	18
C19	18	23	20	16
C20	18	21	22	23

Table 2: Candidates and their marks for group 3

Candidates / Designations	TM	HRM	FM	PDM
C21	21	22	23	16
C22	16	21	20	19
C23	18	16	18	23
C24	15	21	20	24
C25	14	16	23	21
C26	19	24	15	14
C27	24	18	15	22
C28	22	17	21	16
C29	14	15	18	25
C30	13	19	22	24

Table 4: Candidates and their marks for group 4

Candidates / Designations	TM	HRM	FM	PDM
C31	15	18	22	19
C32	21	16	24	20
C33	23	12	19	16
C34	24	19	18	20
C35	21	25	16	24
C36	13	20	17	19
C37	15	24	18	16
C38	13	20	19	17
C39	23	18	22	16
C40	20	16	12	25

Table 3: Candidates and their marks for Group 5

Candidates / Designations	TM	HRM	FM	PDM
C41	16	14	20	22
C42	18	20	21	24
C43	24	21	18	16
C44	23	16	19	14
C45	19	20	12	15
C46	12	16	21	13
C47	18	13	20	10
C48	13	14	22	12
C49	18	11	15	20
C50	24	21	15	10

Final selected 20 candidates after performing first stage (written test) and on performing Hungarian Method-

- TM: C9, C15, C27, C34, C43
- HRM: C3, C13, C26, C35, C50
- FM: C6, C11, C21, C32, C48
- PDM: C8, C14, C29, C40,C42

At *third stage*, selected candidates for each designation were gone through to an interview session which has three qualifying criteria Q1, Q2 and Q3 (which can be named as per the need of the particular designation). In this interview session, candidates were evaluated in terms of linguistic variables of fuzzy logic (table7). Then this result is converted into numeric values by referring the triangular fuzzy values for linguistic values defined in table 6[18].Then in table 8 marks or values are assigned on the basis of table 7 and their corresponding value from table 7.Table 7 and 8 shows corresponding results of this stage for TM designation. Further calculations in the following section will be performed on table 8.

Table 8: Assignment of values based on table 6

	Q1	*Q2*	*Q3*
C9	4	24	15
C15	24	26	12
C27	24	12	24
C34	21	18	26
C43	24	15	12

Table 7:Linguistic variable assignment for TM

	Q1	*Q2*	*Q3*
C9	*VL*	*H*	*M*
C15	*H*	*VH*	*LM*
C27	*H*	*LM*	*H*
C34	*LH*	*HM*	*VH*
C43	*H*	*M*	*LM*

Table 4: The Linguistic variable values

	LinguisticVariable	*TriangularFuzzyNumber*	*WholeValue*
1	*VeryLow(VL)*	(1,1,2)	4
2	*Low(L)*	(1,2,3)	6
3	*HighLow(HL)*	(2,3,4)	9
4	*LowMedium(LM)*	(3,4,5)	12
5	*Medium(M)*	(4,5,6)	15
6	*HighMedium(HM)*	(5,6,7)	18
7	*LowHigh(LH)*	(6,7,8)	21
8	*High(H)*	(7,8,9)	24
9	*VeryHigh(VH)*	(8,9,9)	26

Section 2-

Genetic algorithm Implementation-Here, Genetic algorithm is applied on all the designation clusters found at second stage. In further explanations, Genetic implementation for only TM designation is shown-

1. Chromosome Representation- Normally in genetic representation, binary encoding is used for representing chromosomes. But for the sake of our problem, authors had used value encoding for representing chromosomes. In value encoding, the genes of chromosomes can be represent by real numbers and sequence of values.
2. Fitness Value Calculation- Fitness value is used for deciding the suitability of a particular chromosome and to find its closeness to the optimal solution. For the calculation of fitness value, we used table 8. For calculating fitness value, a fitness function is also required. Table 9 shows the calculated fitness value for each chromosome or candidate. The fitness function used here is –

$$\text{Fitness value} = \left(\sum_{i=1}^{n} Chromosome's\ gene\ value - 1\right)$$

Table 9- Fitness Value Calculated

Chromo some Set	*Fitness Value*
$C9:4,24,15$	42
$C15:24,26,12$	61
$C27:24,12,26$	59
$C34:21,18,26$	64
$C43:24,15,12$	50

3. **Chromosome Selection Method-** For letting our solution close to optimal solution, we have to select best chromosome for further calculation. There have been many selection methods described so far. Here we used rank selection method, after calculating fitness value, chromosomes are sorted in decreasing order, and best ranked chromosomes are selected. Rank 5 is better than 1. Table 10 shows the results of rank selection method.

Table 10- Calculation of rank of each chromosome or

Chromosome Set	*Fitness Value*	*Rank*
$C34:21,18,26$	64	5
$C15:24,26,12$	61	4
$C27:24,12,24$	59	3
$C43:24,15,12$	50	2
$C9:4,24,15$	42	1

4. **Crossover-** As in this paper value encoding is used for chromosome representation, authors had decided to use arithmetic crossover operator. Arithmetic crossover operator produces two new offspring according to equation-

- Offspring 1: a*parent1+ (1-a)*parent2
- Offspring 2: (1-a)*parent1+ (a)*parent2

For performing crossover, authors have divided five chromosomes in three sets. In set A, C34 and C15 has taken, in set B C27 and C43 has taken and in set C, C9 has taken. Table 11 shows the values after performing arithmetic crossover on set A. Similarly, crossover operator can be performed on other sets.

Table 11- Crossover Results

Before Crossover	After Crossover
C34 : 21,18, 26	C34 : 22.2, 21.2, 20.4
C15 : 24,26,12	C15 : 22.8,22.8,17.6

5. **Mutation** – Mutation is used to preserve diversity in chromosome population by finding new dimensions in search space to evaluate. Here, authors used boundary mutation operator, in which upper or lower bound of range gets selected for replacing the value of selected gene. Here, the range is 0-26 and 26(upper limit) was selected to replace the middle gene. Table 12 shows the results of mutation.

Table 12- Mutation Results

Before Mutation	After Mutation
C34 : 22.2,21.220.4	C34 : 22.2,26,204
C15 : 22.8,22.817.6	C15 : 22.8,26,176

After performing all these stages up to one iteration value of each chromosome is calculated again and best three chromosomes (on the basis of their fitness value) get evicted from the population as best chromosomes. The best two candidates for the post of technical manager are C27 and C34. Table 13 shows these results.

Table 13- Final Results for the TM post

Chromosome (Candidate)	Fitness Value
C9	44
C15	65.4
C27	68.2
C34	67.6
C43	65.8

Similarly, the whole procedure can be performed for the posts of HRM,FM and PDM and best candidates can be selected. Table 14 shows final results (candidates selected) for all posts.

Table 14-Finally selected candidates for all posts

Post	*Candidates*	*Fitness Values*
TM	*C27, C34*	68.2,67.6
HRM	*C35, C13, C3, C50*	70.2,68.8,65.8,65.2
FM	*C32, C11, C48*	67,66,65.8
PDM	*C42*	69.6

5 Conclusion

The above process used for the delegation of job field to various candidates has been solved by Fuzzy Linguistic variables and Hungarian method using Genetic approach. This paper results in a sense that fuzzy logic with Genetic algorithm approach results in a far better and accurate way. The method used in this paper is a phased method that continuously refines the results at every phase or stage and finally gives more precise results. This approach is also useful for solving transportation problem, network flow problem etc.

6 No Conflict Declaration

The authors declare that there is no point of conflicts between authors about publishing the paper.

REFERENCES

[1] Kuhn, H.W., "The Hungarian Method for the Assignment Problem", Naval Research Logistics Quarterly, 2:83-97, 1995.

[2] S. P. Eberhardt, T. Duad, A. Kerns, T. X. Brown, A. P. Thakoor, "Competitive Neural Architecture for Hardware Solution to the Assignment Problem", Neural Network, 4(4), 431-442, 1991.

[3] D. Avis, L. Devroye, "An Analysis of a Decomposition Heuristic for the Assignment Problem", Oper. Res.Lett., 3(6), 279-283, 1995.

[4] Lin. Chi-Jen, Wen Ue-pyng, "A Labelling Algorithm for the Fuzzy Assignment Problem", Fuzzy Sets and Systems, 373-391, 2004.

[5] M. S. Chen, "On a Fuzzy Assignment Problem", Jamkang Journal 22(1985), 407-411.

[6] Long-Sheng Huang, Li-Pu Zhang, "Solution Method for Fuzzy Assignment Problem with Restriction of Qualification", Proceedings of the Sixth International Conference on Intelligent Systems Design and Applications (ISDA'06), 2006.

[7] Liu. L., Gao X, "Fuzzy Weighted Equilibrium Multi-Job Assignment Problem and Genetic Algorithm", Applied Mathematical Modelling 33(2009), 3926-3935.

[8] Ye. X, Xu J, "A Fuzzy Vehicle Routing Assignment Model with Connection network based on Priority based Genetic Algorithm", World Journal of Modelling and Simulation 4(2008), 257-268.

[9] S. J. Chen, S. M. Chen, "Fuzzy Risk Analysis on the Ranking of Generalized Trapezoidal Fuzzy Numbers", Appl. Intell. 26(2007), 1-11.

[10] S. M. Chen, J. H. Chen, "Fuzzy Risk Analysis based on the Ranking Generalized Fuzzy Numbers with Different Heights and Different Spreads ", Expert Syst. Appl. 36(2009), 6833-6842.

[11] S. m. Chen, C. H. Wang, "Fuzzy Risk Analysis based on Ranking Fuzzy Numbers using α-cuts, brief features and Signal/Noise ratios", Expert Syst. Appl. 36(2009), 5576-5581.

[12] C. B. Chen and C. M. Klein, "A Simple Approach to Ranking a Group of Aggregated Fuzzy Utilities", IEEE Trans. Syst., Man, Cybern. B, Vol. SMC-27, pp. 26-35, 1997.

[13] F. Choobinesh and H. Li, "An Index for Ordering Fuzzy Numbers", Fuzzy Sets and Systems, Vol. 54, pp. 287-294, 1993.

[14] P. fortemps and M. Roubens, "Ranking and De-fuzzification Methods based Area Compensation", Fuzzy sets and Systems, Vol. 82, pp. 319-330, 1996.

[15] S. H. Chen, "Ranking Fuzzy Numbers with Maximizing Set and Minimizing Set", Fuzzy Sets and Systems,17(1985), 113-129.

[16] R. Sivaraj and Dr. T. Ravichandran, "A Review of Selection Methods in Genetic Algorithm", International Journal of Engineering science and Technology, Vol.3 ,pp.3792-3797,2011.

[17] D.E.Goldberg, "Genetic Algorithms in Search, Optimization and Machine Learning", Addition Wesley,2003.

[18] M. Zaki Ramadan, "Effective Staff Selection Tool: Fuzzy Numbers and Memetic Algorithm Based Approach ", International Jour

TNC Transactions on Networks and Communications
SOCIETY FOR SCIENCE AND EDUCATION UNITED KINGDOM
VOLUME 3, ISSUE 3
ISSN: 2054 - 7420

Li-Fi the future of Vehicular Ad hoc Networks

[1,2]Diyar Khairi M S and [1]Amine Berqia
[1]DEEI, University of Algarve, Portugal
[2]University of Duhok UoD, Iraq
dk.19380@gmail.com; berqia@gmail.com

ABSTRACT

VANET is a set of vehicles moving on the road, equipped with communication capabilities among one to another and with Road Side Units using wireless technologies such as Wi-Fi or WiMAX. The number of possible applications of VANETs is expanding. In addition to safety applications, vehicles are foreseen to support entertainment applications such as peer-to peer applications and Internet connectivity applications. For all this, most mobile data traffic is consumed. Light fidelity (Li-Fi) which is related to visible light communication (VLC) offers many key advantages, and effective solutions. This paper presents some advantages that can improve performance of VANETs by using Li-Fi which is interesting to reach high speed data communication between vehicles.

Keywords: VANETs Vehicular ad hoc networks, Li-Fi Light Fidelity, VLC Visible light communication.

1 Introduction

Nowadays, the need of users to access Internet anywhere at any time is increasingly becoming a necessity. The exponential increase in mobile data traffic has led to the massive deployment of wireless systems. As a consequence, the limited available RF spectrum is subject to an aggressive spatial reuse and co-channel interference has become a major capacity limiting factor. Therefore, there have been many independent warnings of a looming “RF spectrum crisis” as the mobile data demands continue to increase while the network spectral efficiency saturates despite newly-introduced standards and great technological advancements in the field. It is estimated that by 2017, more than 11 exabytes of data traffic will have to be transferred through mobile networks every month [7]. Most recently, VLC has been identified as a potential solution.

Unlike other wireless environments that are mostly stationary or with low mobility, data transmission in VANETs poses more challenges to be resolved. Since the topology is constantly changing, vehicles could move away from their home network and cause connectivity breakage. In order to cope with this problem, a vehicle connected to the wireless network should be able to move using different access points available along the road. These access points could belong to different networks or wireless technologies like Wi-Fi, WiMAX or 3G. The performances are not enough good with the traditional RF technologies. In this paper we will show how in VANETs networks a Li-Fi wireless network would complement existing heterogeneous RF wireless networks, and would provide significant spectrum relief by allowing cellular and wireless-fidelity (Wi-Fi) systems to off-load a significant portion of wireless data traffic.

The reminder of this paper is organized as follows. We start in section 2 with describing VANETs architecture, characteristics, applications and their challenging issues. In section 3, we introduce Li-Fi: the networked, mobile, high-speed VLC solution for wireless communication. In section 4, we focus

DOI: 10.14738/tnc.33.1223
Publication Date: 02nd June 2015
URL: http://dx.doi.org/10.14738/tnc.33.1223

on how Li-Fi can improve QoS and Security requirements for VANETs. Then, we conclude the paper in section 5.

2 Vehicular Ad hoc Networks

Vehicular communication networks have emerged as a key technology for next-generation wireless networking. The main goal of these wireless networks consists in providing safety and comfort for passengers by preventing vehicles crashes and traffic jam. In [1], the authors described vehicular Ad Hoc Networks: (VANETs) can be defined as a form of ad hoc networks to provide communications among nearby vehicles and between vehicles and nearby fixed equipments. VANET is a technology that uses moving vehicles as nodes in a network to create a mobile network. Vehicles which are members of a VANET share information about road conditions via Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) wireless communications.

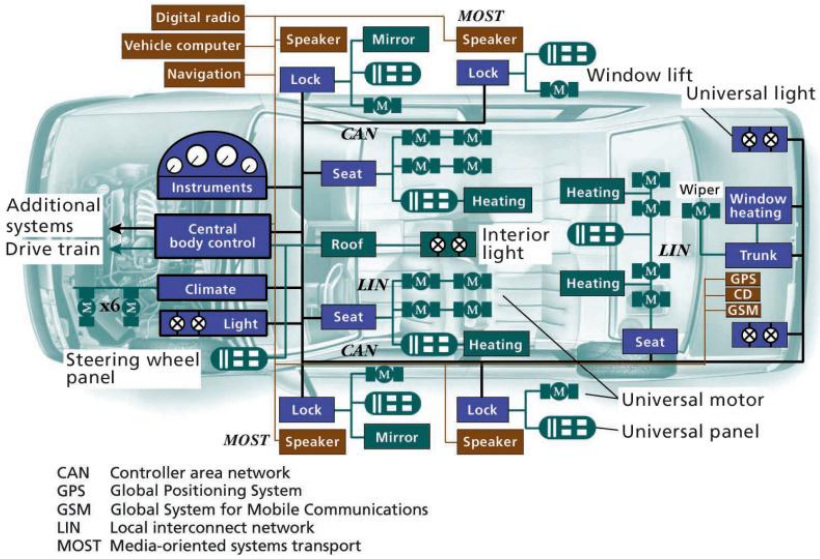


Figure.1 Design of a modern vehicle's network architecture, [4].

2.1 Architecture

This category of wireless networks does not rely on any central control unit and enables vehicles to intelligently communicate with each other and with roadside infrastructure. Each vehicle that is part of a VANET is equipped with an On Board Unit(OBU) and a set of sensors to collect and process information about road conditions, vehicle's position, speed, direction, etc, then send it as a message to other vehicles or RSU through the wireless medium using broadcast communication. The main functions of an OBU are: wireless radio access, ad hoc and geographical routing, network congestion control, IP mobility, reliable message transfer and data security [2].VANETs allow vehicles equipped with OBUs to share information through Vehicle to Vehicle communications (V2V) and to perform communications between vehicles and Road Side Units (RSUs) through Vehicle to Infrastructure communications (V2I). The RSUis equipped with one network device for a Dedicated Short Range Communication for Wireless Access Technology for Vehicular Environment(DSRC//WAVE),developed by the IEEE 1609 Group, which utilizes IEEE 802.11p, a modified version of IEEE 802.11 (Wi-Fi) standard.The motivation behind deployment of DSRC is to enable collision prevention applications (Figure.2).

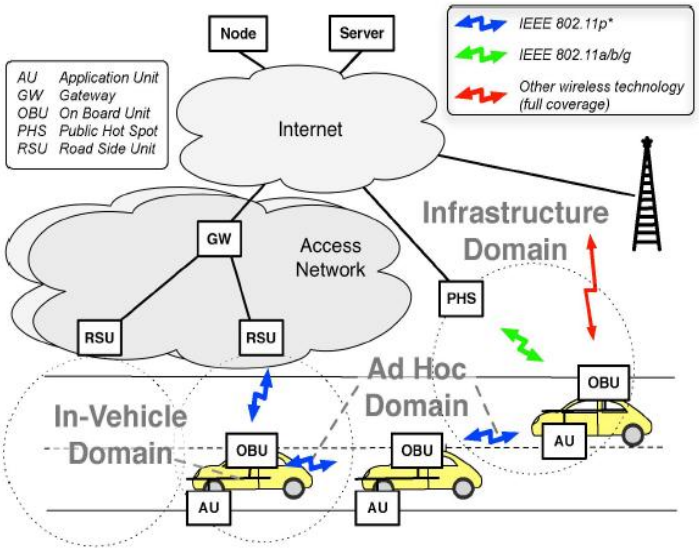


Figure 2. System architecture, currently assumed by the V2V Communication Consortium (C2C-CC) [2]

These applications depend on frequent data exchanges among vehicles, and between vehicles and roadside infrastructure [3].RSU is responsible about extending the communication range of the ad hoc network by re-distributing the information to other OBUs and by sending the information to other RSUs in order to forward it to other OBUs, running safety applications such as a low bridge warning, accident warning or work zone, using Infrastructure to Vehicle communication (I2V) and acting as a source of information and providing Internet connectivity to OBUs [2]. The OBU is connected to other OBUs or RSUs trough a wireless link based on IEEE 802.11p radiofrequency channel. OBU can also communicate with other hosts for non-safety applications, using the communication of cellular radio networks (GSM, GPRS, UMTS, HSDPA, WiMAX and 3G or 4G).

Characteristics

VANETs have individual characteristics that are decisive in the design of the communication system. These include: dynamic topology, large scale network, high computational capability, impredictiblemobility, infinite energy supply in order to provide real time message dissemination platform to share data between vehicles and guarantee reliable exchange of information.

Infinite energy supply: vehicles in VANETs are not energy constrained like are nodes in a MANET. The vehicle can provide energy to the OBU continuously via the long life battery.

Rapid changes in the network topology:due to the high speed of vehicles, the topology of the network is very dynamic. VANETs will not have constant connectivity because of the high-speed movement between vehicles. In low-density vehicles, the link is highly likely to be disconnected.

Predictable mobility: unlike MANET where nodes move in a random way, VANET topology is not absolutely random. VANET movement restrictions are defined by road layout, topology, traffic rules, and the reaction to messages sent by other vehicles.

High computational capability: Because the nodes in VANET are vehicles, they can be equipped with a sufficient number of sensors and computational resources; such as processors, a large memory capacity, advanced antenna technology and global position system (GPS).

2.2 Applications

The three major classes of VANETs applications are safety applications, convenience applications and commercial applications [13, 14, 15]. For example, applications like collision alert, weather conditions, road surrounding warning are classified under safety applications. They use the message broadcast feature of VANETs to inform nearby vehicles about critical alerts. Convenience applications would detect road congestion, help tool booths to collect toll without stopping vehicles. These applications are classified as safety applications which aim to ameliorate traffic conditions and prevent road accidents and save peoples' lives.

Commercial and entertainment applications become an attractive tendency. They include a wide range of future multimedia and data applications, such as audio/video as well as e-maps and roads vehicle related services. Road side businesses such as hotels and restaurants can use content rich video streams to broadcast advertisements to drivers on the road. Peer-to-peer applications are another category of non-safety VANET applications. Passengers in nearby cars can set up a video conversation by using the inter vehicle streaming technology, exchange music, instant messages, stream music or movies from special servers. Travelers could play games in order to alleviate boredom. Vehicles are envisaged to become a part of internet in the near future, either as mobile endpoints, as mobile backbone routers or as mobile sensors.

2.3 Challenges

VANETs inherit from the wireless network shortcomings since they use radio frequency channel to exchange information between the different entities composing the network. These shortcomings consist on signal fading and bandwidth limitations [22].

Signal fading: This phenomenon is mainly frequent in urban regions. Buildings or other vehicles may constitute obstacles for nodes communications. These objects may cause transmitted signal fading or prevent it from reaching its destination.

Bandwidth limitations: as mentioned before, VANETs do not rely on any central administration. Consequently, this brings out problems about the management of nodes communication and contention control. In order to optimize vehicular communications, it is necessary to use the available bandwidth efficiently. The high density of vehicles in urban regions may increase the probability of channel contention. An efficient utilization of the available bandwidth influences the time delay of message dissemination. Channel contention increases data transmission latency. This has very negative impacts, especially for warning messages delivery in safety applications. For entertainment applications, channel contention and the non-optimal use of bandwidth causes degradation of QoS requirement of users.

In addition there are some challenges which are specific for VANETs. Some of these challenges are time constraints, large scale of the network, and high mobility of nodes [20].

Time constraints: Safety messages are critical information which should be delivered with respect to time limitations. Warning messages are very time sensitive, so they must be delivered in a short interval of time beyond which they are useless. A driver must have enough time to react to a received warning message in order to prevent a crash.

Large scale network: the growing number of vehicles on the road will become, in the near future, one on the main constraints facing VANETs. A global authority must be set to manage information about users and others related to security. Since the security and privacy rules differ from a region to another in the world, their standardization will be complicated.

High mobility of nodes: VANETs are characterized by high topology changes due to the high speed of vehicles. These changes cause frequent link failures. To alleviate this problem it is necessary to elongate link life by increasing the transmission power. But this solution can cause throughput degradation[9]. The vehicles high speed may cause handoff and cause packets loss which can reduce the throughput of the network. Since vehicles frequently change their point of network attachment when they access Internet services, they need mobility management schemes that provide seamless communication. This mobility management meets requirements such as seamless mobility, support IPV6, scalable overheads and low handoff latency. One approach for mobility management recently proposed NEMO Basic Support. VANETs differ from MANETs in the highly mobile nodes, the probability of network partition which is higher and end-to-end connectivity which is not guaranteed.

Privacy and security: VANETs are very constrained in terms of security and privacy. Making a balance between security and privacy to protect, users and data, in the same time, is a key challenge which must be solved. While registration to the network, vehicles provide some credentials because users require trustworthy information. However, this may violate source privacy.

3 Li-Fi

Visible light communication (VLC), which uses a vast unregulated and free light spectrum, has emerged to be a viable solution to overcome the spectrum crisis of radio frequency. Light fidelity (Li-Fi) is an optical networked communication in the subset of VLC to offload the mobile data traffics.

During the last ten years, there have been continuous reports of improved point-to-point link data rates using off-the-shelf white LEDs under experimental lab conditions. Recently, data rates in excess of 1 Gbps has been reported using off-the-shelf phosphor-coated white LEDs,4 and 3.4 Gbps has been demonstrated with an off-the-shelf red-green-blue (RGB) LED. To the best of the authors' knowledge, the highest speed that has ever been reported from a single color incoherent LED is 3.5 Gbps. The experiment was led by researchers of the University of Edinburgh. VLC, and the Li-Fi Consortium was formed in Oslo, Norway in 2011 with the purpose of providing a high speed and wireless optical network [11,12].The vision is that a Li-Fi wireless network would complement existing heterogenous RF wireless networks, and would provide significant spectrum relief byallowing cellularand wireless-fidelity (Wi-Fi) systems to off-load a significant portion of wireless data traffic.

Unlike RF modulation methods, VLC adopts the intensity modulation to carry binary data by turning LED on and off quickly, in which the amplitude and phase information are lost. For providing both illumination and seamless communication coverage, attocell architecture has been proposed, which is referred from cellular network as the cell sizes are smaller than in a typical RF femtocell network. Every LED light bulb in attocell Li-Fi network is treated as an access point and an illumination source for covering a limited region. In this context, Li-Fi is shown potentially to provide at least an order of magnitude improvement in the area spectral efficiency (ASE) as compared to the femtocell system [8].

In attocell Li-Fi architecture like RF cellular network, inter-cell and intra-cell interference mitigation techniques are indispensable. The most common method is to assign different sub-bands for neighboring cells in order to avoid co-channel interference (CCI). A combined wavelength division and code division scheme is proposed in [10].

4 Li-Fi & VANETs

In this section we propose our VANET architecture based on Li-Fi. Based on the attocell architecture, users must be associated with one or some cars LED lamps for accessing and downlink transmission. The enhanced bandwidth-based (BB) lamp selection scheme [6] access scheme is used.

Enabling communications in mobile outdoor systems, particularly in dense, fast moving safety-critical automotive environments is one of the main benefits of VLC for VANETs. In vehicular applications, mobile communications are particularly suitable for adoption of directional communications using Line Of Sight LOS links. Applications such as safety and emergency messaging require very high reliability, and this can be provided through short-range inter-vehicular communications. As an instance, vehicles can be equipped with optical transceivers, such that they can communicate with other similarly equipped vehicles. Together with adaptive cruise control assisted by V2V communications, the problem of vehicle crashes due to human error can be alleviated.

Figure 3. Li-Fi for V2V communications

Our attention will be focused on the use of Visible Lighting Communications (VLC) Li-Fi and how it can provide a valid technology for communication purposes in VANETs. The use of the visible spectrum provides service in densities exceeding femtocells for wireless access. It represents a viable alternative that can achieve high data rates, while also providing illumination. This configuration minimizes packet collisions due to Line Of Sight (LOS) property of light and promises to alleviate the wireless bottleneck that exists when there is a high density of rich-media devices seeking to receive data from the wired network.

We present in figures 4 and 5 the results of our experiments using Matlab [23]. For all experiments, we consider two cars which start at the same time and with the same speed. We evaluate the latency and the average packet loss ratio using three velocities 50 km/h, 70 km/h and 90 km/h and with different distances between cars. We consider UDP traffic between nodes with 2048 kbps. In figures 4 and 5 we can see the latency and the packet loss ratio.

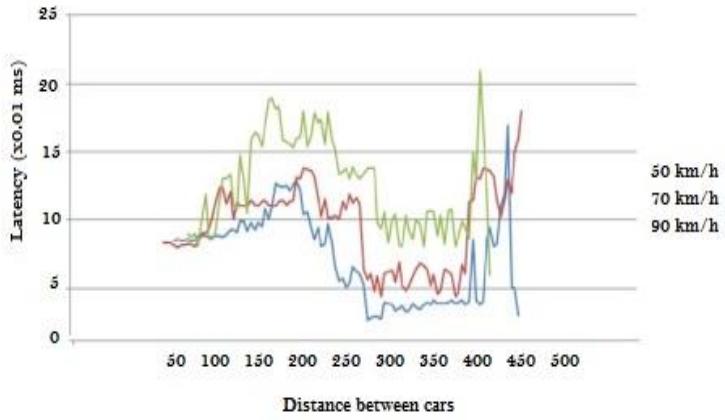


Figure 4. Latency for 2 cars

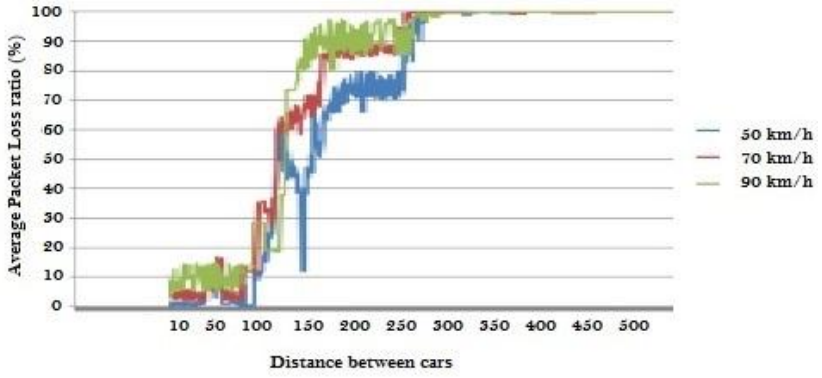


Figure 5. Packet Loss ratio for 2 cars

Based on the results we can that the latency using Li-fi communication between cars is around 0.02 ms which is better than the latency using the standard IEEE802.11p [24]. For the packet loss ratio, we have the confirmation that when the distance between cars increases the packet loss ratio increases till 100% when the cars are very far one from the other.

5 Conclusion

In this paper we investigated main aspects of vehicular ad hoc networks. We discussed the state of art research on Li-Fi and its potential advantages that can make it supplement RF communications and improve wireless network performance wherever short range links are used such as vanets for high speed and secure data transmission. However, there are still many problems that need additional study. The cooperative techniques and protocols between Li-Fi and the existing RF network need further study. RF networks are widely used and gradually to be indispensable in our lives. Integrating Li-Fi into RF communications will not only accelerate the marketization of Li-Fi, but also offload traffic from the extremely crowded cellular networks. However, a large number of feedback packets and considerable delay may exist when performing handover between Li-Fi and RF network, which need to be investigated.

REFERENCES

[1] Sasha Dekleva, J.P. Shim,UpkarVarshney, and Geoffrey Knoerzer “Evolution and emerging issues in mobile wireless networks”, ACM Communications Vol. 50, No. 6, June 2007.

[2] C.C. Communication Consortium; IEEE trial-use standard for wireless access in vehicular environments; Olariu and Weigle, 2009.

[3] John B. Kenney, Dedicated Short-Range Communications (DSRC) Standards in the United States, Proceedings of the IEEE | Vol. 99, No. 7, July 2011.

[4] G Leen, D Heffernan, Expanding Automotive Electronic Systems, Computer, 3518893Jan. 2002

[5] S Dornbush, A Joshi, Street Smart Traffic: Discovering and Disseminating Automobile Congestion using VANETs, In Proc. of the IEEE VTC, Spring, April 2007.

[6] Huang, Z. T., &Ji, Y. F. (2012). Efficient user access and lamp selection in LED-based visible light communication network. Chinese Optics Letters, 10(5), 050602(1–5).

[7] Cisco Visual Networking Index, "Global Mobile Data Traffic Forecast Update, 2012-2017," White Paper, CISCO (Feb. 2013).

[8] Stefan, I., Burchardt, H., & Haas, H. (2013). Area spectral efficiency performance comparison between VLC and RF femtocell networks. In 2013 IEEE international conference on communications (ICC), pp. 3825–3829

[9] Saif Al-Sultan, Moath M.Al-Doori, Ali H. Al-Bayatti, Hussien Zedan, A comprehensive survey on vehicular Ad Hoc network, Journal of Network and Computer Applications 37 (2014) 380–392.

[10] Cui, K. Y., Quan, J. G., & Xu, Z. Y. (2013). Performance of indoor optical femtocell by visible light communication. Optics Communications, 298, 59–66.

[11] Visible Light Communications Consortium. http://www.vlcc.net/

[12] Li-Fi Consortium. http://www.lificonsortium.org/

[13] Kamini, Rakesh Kumar, "VANET parameters and applications: A review", Global Journal of Computer Science and Technology, vol. 10 issue 7 p 72-77, September 2010.

[14] B. Mishra, P. Nayak, S. Behera, D. Jena, "Security in Vehicular Ad hoc Networks: A survey", ICCCS, February 2011, ACM, Pages 590-595.

[15] C.-T. Li, M.-S.Hwang and Y.-P. Chu, "A Secure and Efficient Communication Scheme with Authenticated Key Establishment and Privacy Preserving for Vehicular Ad Hoc Networks". Computer Communications, Volume 31, Issue12, 30 July 2008, Pages 2803-2814.

[16] T. Leinmuller, R.K. Schmidt, E. Schoch, A. Held, G. Schafer, Modeling roadside attacker behavior in VANETs, in: GLOBECOM Workshops, IEEE, New Orleans, LO, 2008, pp. 1–10.

[17] HartensteinH, Laberteaux K P. A tutorial survey on vehicular ad hoc networks. Communications Magazine, IEEE 2008; 46(6): 164–71.

[18] David Hiebeler, http://cran.r-project.org/doc/contrib/Hiebeler-matlabR.pdf, May 25, 2010

[19] D. Jiang, L. Delgrossi, "IEEE 802.11p: towards an international standard for wireless access in vehicular environments", IEEE Vehicular Technology Conference (VTC-Spring) (2008), pp. 2036 – 2040

TNC Transactions on Networks and Communications
SOCIETY FOR SCIENCE AND EDUCATION UNITED KINGDOM
VOLUME 3, ISSUE 3
ISSN: 2054 - 7420

Android Application Development for Secure Data Transmission using Steganography

[1]Vineet Ramesh Jeswani, [2]Savita Kulkarni and [3]Manisha Ingle
Department of Electronics and Telecommunication, Maharashtra Institute of Technology, Pune, India
[1]vineetjeswani26@gmail.com; [2]savita.kulkarni@mitpune.edu.in; [3]manisha.ingle@mitpune.edu

ABSTRACT

Real time implementation of Steganographic algorithm along with encryption is used to achieve secure data flow across Android mobiles. In this paper, pixel value differencing (PVD) technique one of the steganographic algorithm with AES encryption are implemented using JAVATM on android platform to achieve high level security for real time multimedia messaging service (MMS) system. One of the important concerns in any communication system is the security of the data transmission from eavesdropper. To overcome this security problem, the most effective technique is the steganography. Steganography is used to hide secret information onside some carrier. Image is taken as a carrier file to hide secret information (text, image, audio). To add more security, encryption is also done on the secret file which will be hidden inside MMS. The Pixel Value Differencing (PVD) technique is used to hide secret information (text, image, audio). Different sizes of secret images are considered keeping the fixed size of cover image and the calculations have been done for MSE and PSNR of image in MATLAB. Later, the results of the PVD are compared with the LSB technique. Encryption and Steganographic algorithms are ported on Sony Xperia M mobile device with Android version 4.3.

Keywords – Android Platform, Encryption, LSB, PVD, MMS, MSE, PSNR, Security, Steganography.

1 Introduction

The basic purpose of mobile is communication. Over the last few decades mobile phones have evolved very rapidly. Earlier, mobiles where used to communicate via voice call only. Later, came the era of the GSM mobile phones in which communication was possible through short messaging service (SMS) which used the text format to communicate and it became very popular among users. With more evolution, communication became possible through multimedia messaging service (MMS) in which communication became possible via text, audio, image and video. MMS is a technology that allows a user of an enabled mobile phone to create, send, receive and store messages that include text, images, audio and video clips properly. Today is the era of smart phones where various operating systems are available such as Android, Windows, Blackberry, IOs and many more with various features. With this ever growing technology, security has become an important subject and has gained increasing importance. The security with Android is least as compared with other OS currently available in the market. Moreover, android is an open source and free platform where a developer can create its own application and share it on play store with users. Users can explore the play store and can get the required applications very easily and most of the applications are freely available. Adding to many advantages of Android, more than 80% of the smart phone users prefer Android over others. Due to all this reasons, we have selected Android to achieve MMS security. To achieve the security various techniques are available such as encryption, cryptography, steganography. The best suitable and the

DOI: 10.14738/tnc.33.1292
Publication Date: 27th June 2015
URL: http://dx.doi.org/10.14738/tnc.33.1292

most secured technique is the steganography. Steganography is the art of hiding the secret data over the cover medium. There are many advantages of steganography over other techniques. Even in the steganography techniques, there are various algorithms such as Least Significant bit (LSB) algorithm, Pixel value differencing scheme (PVD) algorithm and many more. The LSB-based technique, directly embed the secret data into the spatial domain in an unreasonable way without taking into consideration the difference in hiding capacity between edge and smooth areas. In general, the alteration tolerance of an edge area is higher than that of a smooth area, this meaning that, an edge area can conceal more secret data than a smooth area. While human perception is less sensitive to subtle changes in edge areas of a pixel, it is more sensitive to change in the smooth areas. While in case of the PVD technique, the correlation between neighboring pixels to determine whether a pixel is located in an edge area or a smooth area, the PVD method does not utilize the smooth area to hide large amount of secret data, the capacity is still low. In order to achieve higher capacity, a combination of PVD and LSB can be used. These techniques are based on the idea of using PVD when the difference between a pair of pixels is large (edge area), and using LSB method when the difference is small (smooth area). To add further more security, along with these steganographic techniques, encryption is also done on the secret file in which a hiding data will be encrypted with a secret key which will be available to both sender and receiver so that it can be used while retrieving the secret data at the receiver's end.

2 Problem Definition

The aim of the project is to hide the data as an image or text over an image from MMS using pixel value differencing steganographic algorithm and before hiding, an image performs encryption on it. Send the stego file to the destination where the retrieving of the hidden data is done on mobile device with Android.

2.1 Problem Solution

Hiding an image over an image has already been achieved using 4-LSB steganography algorithm. But the drawback with this technique is that the cover image should be of .bmp format and the secret image should be of .jpg format. Moreover the efficiency of this technique is low.

To overcome these drawbacks, PVD algorithm is used. The proposed method should provide better security while transferring the data or message(s) from one end to the other end. The main objective of this project is to increase the data hiding capacity and the data transfer efficiency as compared to that of the 4-LSB algorithm hide encrypted secret image into an image from MMS which acts as base file having secret data and to transmit to the destination securely without any modification. If any distortions occur in the image or on its resolution while inserting the secret message into the image, there may be a chance for an unauthorized person to modify the data. So, the data (image, text) encryption at sender and decryption at receiver and steganography plays an important role in this project.

2.2 System Architecture

The data hiding patterns using the PVD stegano-graphic technique in this project can be explained using this simple block diagram which is similar to that used in the previous work where Steganography was achieved using 4-LSB algorithm. The block diagram is kept same because only the steganography is changed i.e. from 4-LSB to PVD as shown in figure 1 and 2. [1]

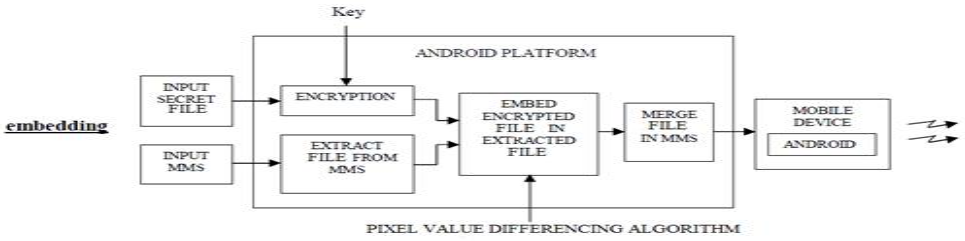


Figure 1 Embedding at Transmitter

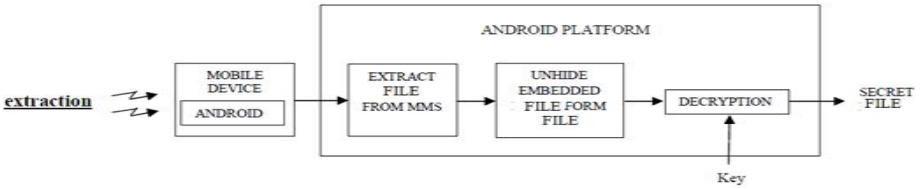


Figure 2 Extraction at Receiver

3 Steganography

In steganography the data are hidden in a cover media so that other persons will not notice that such data is there.

Or Steganography is a technology of hiding messages inside some harmless carriers to shelter the communication so that the outsiders may not discover the existence of information in the carrier. Steganography is mainly applied to media such as images, text, video clips, music and sound.

The different types of steganography techniques that are available are:

1. Pure steganography
2. Secret key steganography
3. Public key steganography

3.1 Pure Steganography

Pure Steganography is the process of embedding the data into the object without using any private keys as shown in Figure. This type of Steganography entirely depends upon the secrecy. This type of Steganography uses a cover image in which data is to be embedded, personal information to be transmitted, and encryption decryption algorithms to embed the message into image. These types of steganography can't provide the better security because it is easy for extracting the message if the unauthorized person knows the embedding method. It has one advantage that it reduces the difficulty in key sharing.

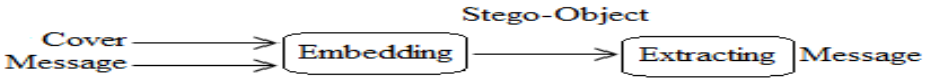


Figure 3 Pure Steganography

3.2 Secret key Steganography

Secret key Steganography is another process of Steganography which uses the same procedure other than using secure keys shown in Figure. It uses the individual key for embedding the data into the object that is similar to symmetric key. For decryption it uses the same key which is used for encryption. This type of Steganography provides better security compared to pure Steganography. The main problem of using this type of steganographic system is sharing the secret key. If the attacker knows the key it will be easier to decrypt and access original information.

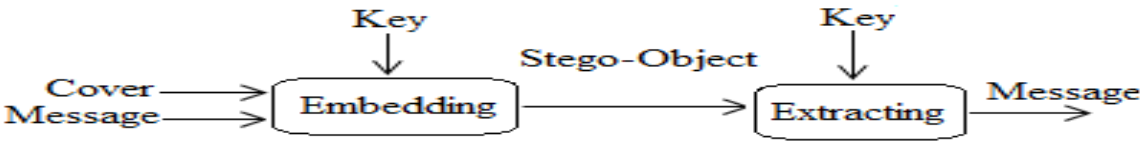


Figure 4 Secret key Steganography

3.3 Public key Steganography

Public key Steganography uses two types of keys shown in Figure. One for encryption and another for decryption. The key used for encryption is a private key and for decryption, it is a 'public key' and is stored in a public database.

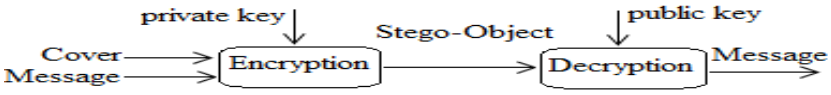


Figure 5 Public key Steganography

4 Image Steganography

Images are the most popular cover objects used for steganography. In the domain of digital images many different image file formats exist, most of them for specific applications. For this different image file formats, different steganographic algorithms exist.

4.1 Lsb technique

The most basic and important image Stegano-graphic Technique is Least Significant Bit embedding tech-nique. In this technique, data can be hidden in the least significant bits of the cover image and the human eye would be unable to notice the hidden image in the cover file. This technique can be used for hiding images in 24-bit, 8-bit or gray scale format. In this technique, least significant bit of each pixel is replaced with secret message bit until message end. When using a 24-bit image one can store 3 bit in each pixel by changing a bit of each if the red, green and blue color components. An 800 x 600 pixel image can store 1,4400,00 bits or 180,000 bytes of embedded data. For example a 24 bit can be as follows:

(10110101 01101100 10101101)
(10110110 11001101 00111110)
(10110101 01100011 10001110)

The number 150 which binary representation is 10010110 is embedded into the least significant bits of this part of the image, the resulting grid as follows:

(10110101 01101100 10101100)
(10110111 11001100 00111111)

(10110101 01100010 10001110)

Although the number is embedded into the first 8 bytes of the grid, only the 3 underlined bits need to be changed according to the embedded message. On an average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size. There are 256 possible intensities of each primary color, so, changing the LSB of a pixel results in small changes in the intensity of the colors. These changes cannot be perceived by the human eye, thus the message is successfully hidden. If the message is hidden even in the second to least significant as well as in least significant bit then too no difference is seen in the image. In LSB Technique, consecutive bytes of the image data from the first byte to the end of the message are used to embed the information. But this approach is very easy to detect. A more secure system can be in which the sender and receiver share a secret key that specifies only certain pixels to be changed. Even if the intruder suspects that LSB steganography has been used, there is no way of knowing which pixels to target without the secret key. In its simplest form, LSB makes use of BMP images, since they use lossless compression. To hide a secret message inside a BMP file, one would require a very large cover image. For this reason, LSB method has also been developed for use with other image file formats. This type of information hiding algorithm could be a major risk because eavesdropper can apply sequential scanning based technique to recover the secret message [1-5].

4.2 Pixel Value Differencing Scheme

Wu & Tsai discuss Pixel Value Differencing (PVD) scheme. This technique takes advantage of the characteristics of human visual system. In this technique, the original cover image is divided into non overlapping blocks of two pixels. A range table with a number of contiguous ranges is fabricated. The width of each range in the table is in power of 2. Now, difference is calculated between two consecutive pixels of a block. The block with large difference value is considered in edge area and with small difference value is considered in smooth area where the small or large values are taken depending upon some pre-specified threshold value. The human eyes are more sensitive to noise in smooth area than in the edge area. This method embeds more bits in edge areas in contrast to smooth areas. This technique doesn't have sufficient embedding capacity. Another technique discussed by Wu, Tsai and Hwang that also exploits the characteristics of the human visual system. In this method, the image is also divided into non-overlapping blocks of two consecutive pixels and then the difference value is calculated for each block in similar way as in. On the basis of the difference value, each block is identified either as a part of smooth region or edge region. This method embeds the secret data bits into the smooth regions by simple LSB substitution method and for edge area the Wu & Tsai's scheme is used. Thus, it increases the data hiding capacity to a great extent without disturbing the image quality much. The methods discussed in identify the horizontal edges only [6-7].

Table 1. Range Table

Range (R)	Lower Bound (LB)	Upper Bound (UB)
R1	0	15
R2	16	31
R3	32	63
R4	64	127
R5	128	255

5 Implementation

The cover images and secret images to send/transfer are stored in the MicroSD card of Android mobile device with android version 4.3 whereas text has to be directly given as a secret file which we want to hide and send. Cover image along with text message is Multimedia Message.

5.1 Embedding Algorithm

1. Start
2. Pick base image as a carrier file from Micro SDcard of Android mobile device.
3. Pick the data to be hidden either text or image or audio.
4. If the data to hide is in text format input it manually.
5. If the data to hide is image search in Micro SDcard.
6. Encrypt the hiding data with AES encryption algorithm.
7. Perform Steganography using Pixel Value Differencing (PVD) algorithm.
8. PVD differentiates smooth area and the edge area and accordingly hides more data in the edge area.
9. Generate an MMS using this Stego image.
10. Send it over Android platform.

The secret file is hidden in the blue channel of the base image. The minimum size of Cover image = 10* Size of Secret image + n (where n is size of cover image header)

n pixels are added because secret data is not be added in the header of cover image; therefore start setting secret data after the header of cover image.

5.2 Extracting Algorithm

Extracting the secret image data is performed by reversing the process used to insert the secret message in the cover image. The following steps describe the details of extraction process.

1. Read Multimedia message.
2. Extract the image from Multimedia message i.e stego
3. image.
4. Separate out the data of the hidden file from the base
5. image by performing stegnalysis.
6. Once the data is completely separated perform decryption on the secret file with the same key used for encryption.
7. Display the hidden file (text or image or audio) from Micro SDcard.

For measuring the quality of reconstructed image as compared to the original image, the metric needs to be define. There are three common error metrics used for estimating noise on images: MSE, PSNR, and SSIM.

6 Result

Evaluation parameters are used Peak Signal to noise ratio (PSNR), Mean Square Error (MSE) as performance parameters to measure the quality of image.

Signal-to-noise ratio can be defined in a different manner in image processing where the numerator is the square of the peak value of the signal and the denominator equals the noise variance. Two of the error metrics used to compare the various image de-noising techniques is the Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR).

6.1 Mean Square Error (MSE):

Mean Square Error is the measurement of average of the square of errors and is the cumulative squared error between the stego and the original image. The error indicates the distortion in an image. MSE can be calculated by using 2-D mathematically equation described as follows:

$$MSE = \left(\frac{1}{N}\right)^2 \sum_{i=1}^{M} \sum_{j=1}^{N} (X_{ij} - \bar{X}_{ij})^2. \quad (1)$$

Where, Xij = The value of pixel in cover image
Xij = The value of pixel in stego image
N = Size of image

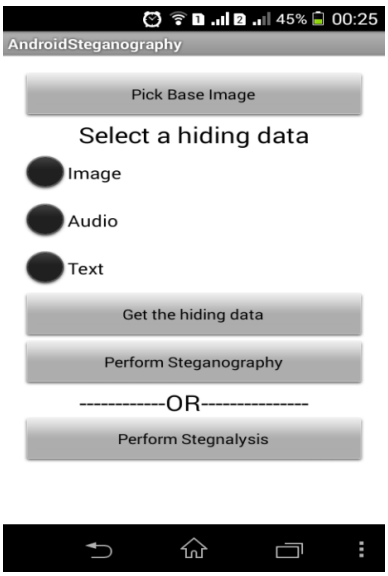
6.2 Peak Signal to Noise Ratio (PSNR):

PSNR is a measure of the peak error. Peak Signal to Noise Ratio is the ratio of the square of the peak value the signal could have to the noise variance as shown in (2).

$$PSNR = 10 \text{ X } \log \frac{255^2}{MSE} \text{ dB} \quad (2)$$

A higher value of PSNR is good because of the superiority of the signal to that of the noise. MSE and PSNR values of an image are between original image and stego image.

6.3 Graphical User Interface (GUI):



Example 1: Hiding image within an image

Base Image

Secret Image

Table 2. Comparison of MSE for Various Sizes of Secret Image: Example 1(Jelly Bean)

Base Image Size	Secret Image Size	MSE using 4-LSB	MSE using PVD
150X203	100X75	3.7269	2.5025
150X203	140X105	4.1079	3.7599
150X203	150X112	4.5364	3.9336
150X203	160X120	4.9885	4.2094

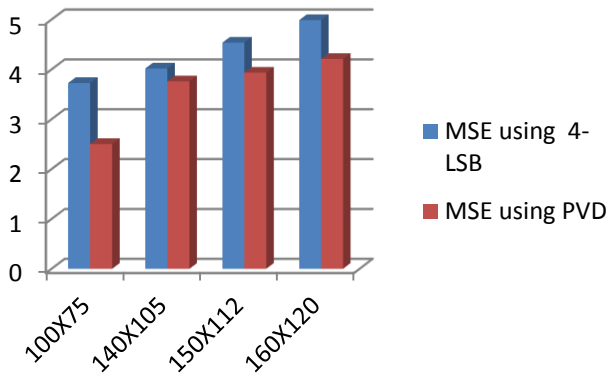
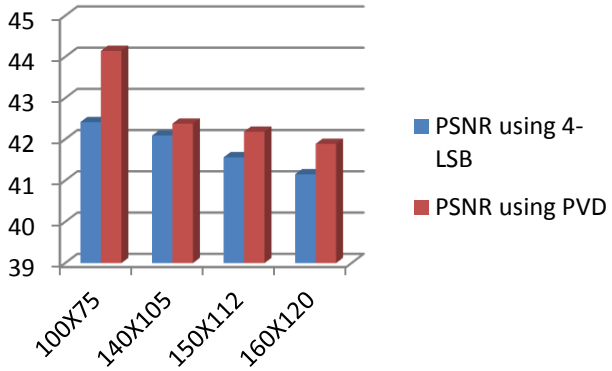


Table 3. Comparison of PSNR for Various Sizes of Secret Image: Example 1(Jelly Bean)

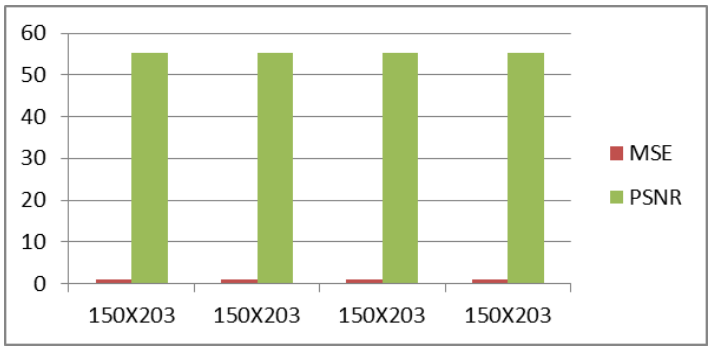
Base Image Size	Secret Image Size	PSNR using 4-LSB	PSNR using PVD
150X203	100X75	42.4173	44.147
150X203	140X105	42.0908	42.3791
150X203	150X112	41.5636	42.1829
150X203	160X120	41.1511	41.8886



Example 2: Hiding text within an image

Table 3. Calculation of MSE And PSNR For Hiding Text

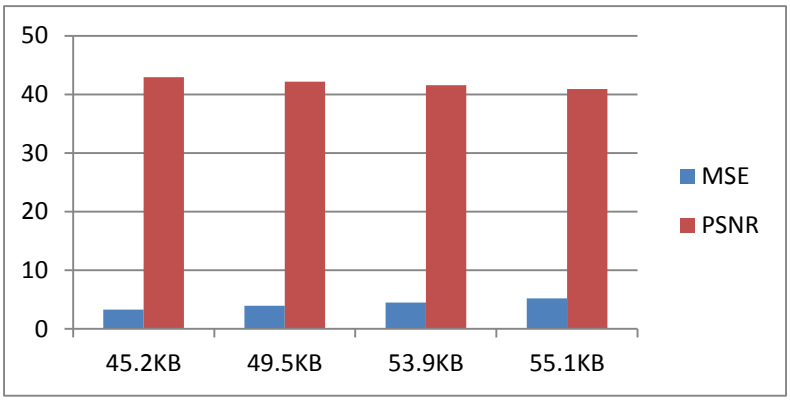
Base Image Size	No of text characters	MSE	PSNR
150X203	20	1.0019	55.3901
150X203	30	1.002	55.3844
150X203	40	1.0023	55.3809
150X203	50	1.0025	55.3744



Example 3: Hiding audio within an image

Table 3. Calculation Of MSE And PSNR For Hiding Audio

Base Image Size	Audio Size	MSE	PSNR
150X203	45.2KB	3.3084	42.9346
150X203	49.5KB	3.9411	42.1746
150X203	53.9KB	4.5217	41.5777
150X203	55.1KB	5.2304	40.9545



7 Conclusion

PVD steganographic algorithm is successfully implemented to hide secret data (image, text) into an image from MMS which provides the security during transmission of MMS. Comparison between PVD and LSB algorithm is done by calculating MSE and PSNR of the Stego images. And the results of PVD are more effective as compared to that of LSB. Moreover, hiding text and audio is also achieved in this project which was not done using LSB algorithm. Algorithm is developed on android platform and testing is done on the actual android mobile device Sony Xperia M with android version 4.3. In this way, AES encryptions along with PVD Steganography algorithm are successfully implemented using Android platform with high potential of security.

ACKNOWLEDGMENT

Authors would like to thank Electronics and Telecommunication Department and the faculty of Maharashtra Institute of Technology, Pune, for their co-operation and the help in completion of this project. Also, I thank all my friends and family members for their appraisal and criticism, which helped me to make my project success.

REFERENCES

[1] Geetanjali R. Kshirsagar, Savita Kulkarni “Implementation of Hybrid Algorithm for Secured Multimedia Messaging Service System Using Android” Proc. of the Second Intl. Conf. on Advances in Computer, Electronics and Electrical Engineering -- CEEE 2013

[2] Mr. Vikas Tyagi “ Data Hiding in Image using least significant bit with cryptography” International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012

[3] Rosziati Ibrahim, Law Chia Kee “MoBiSiS: An Android-based Application for Sending Stego Image through MMS” ICCGI 2012 : The Seventh International Multi-Conference on Computing in the Global Information Technology June 24-29, 2012 - Venice, Italy

[4] S.Mohanapriya "Design and Implementation of Steganography Along with Secured Message Services in Mobile Phones" International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 5, May 2012

[5] Mukesh Garg, A.P. Gurudev Jangra "An Overview of Different Type of Data Hiding Scheme in Image using Steganographic Techniques" International Journal of Advanced Research in Computer Science and Software Engineering. Volume 4, Issue 1, January 2014

[6] Wu D. C and Tsai W. H. (2003), "A steganographic method for images by pixel-value differencing", Pattern Recognition Letters, vol. 24, no. 9-10, pp. 1613-1626.

[7] Wu H.C., et al. (2005), "Image Steganographic scheme based on pixel-value differencing and LSB replacement methods", VISP(152). [8]Marghny H. Mohamed, Naziha M. Al-Aidroos and Mohamed A. Bamatraf "Innovative Multi-Level Secure Steganographic Scheme based on Pixel Value Difference" International Journal in Foundations of Computer Science & Technology (IJFCST), Vol. 2, No.6, November 2012.

TNC Transactions on Networks and Communications
SOCIETY FOR SCIENCE AND EDUCATION UNITED KINGDOM
VOLUME 3, ISSUE 3
ISSN: 2054 - 7420

The Non-Uniform Communication Performance of Adaptive Routing for Hierarchical Interconnection Network for 3D VLSI

[1]Yasuyuki Miura, [2]Shigeyoshi Watanabe, [3]M.M. Hafizur Rahman
[1,2]School of Information Technology, Shonan Institute of Technology, Fujisawa, Japan;
[3]International Islamic University, Malaysia (IIUM), Kuala Lumpur, Malaysia;
miu@info.shonan-it.ac.jp; watanabe@info.shonan-it.ac.jp; hafizur@iium.edu.my

ABSTRACT

The Tori-connected mESH (TESH) Network is a k-ary n-cube networks of multiple basic modules, in which the basic modules are 2D-mesh networks that are hierarchically interconnected for higher level k-ary n-cube networks. Many adaptive routing algorithms for k-ary n-cube networks have already been proposed. Thus, those algorithms can also be applied to TESH network. We have proposed three adaptive routing algorithms - channel-selection, link-selection, and dynamic dimension reversal - for the efficient use of network resources of a TESH network to improve dynamic communication performance.

In this paper, we have evaluated the dynamic performance of a TESH network using different non uniform traffic patterns. In this paper, we have evaluated by local communication traffic pattern in addition to the hotspot, perfect shuffle, and complement traffic patterns. It was shown that the dynamic communication performance was improved when inter-BM communication appeared frequently such as perfect shuffle and local communication traffic patterns.

Keywords: TESH network, adaptive routing algorithm, communication performance

1 Introduction

Interconnection networks are the key elements for building massively parallel computers consisting of hundreds or thousands of processors[1]. Recent progress in very-large-scale integration (VLSI) and network-on-chip (NoC) technology has led to multicomputer systems on three-dimensional LSIs.

Through Silicon Via (TSV) is widely used in 3D-LSI implementation. Like the via of printed circuit board, TSV pierces between silicon chips. By the inter-chip connection through TSV, the complex 3D VLSI implementation can be realized. However, in the LSI structure, large amount of layout area is necessary for inter-chip connection. So, the number of inter-chip connections should be reduced. Using 30-40 nm CMOS gate length, the length of a TSV is several μm. Based on this issue, we have been studied the hierarchical interconnection network which can reduce the number of wires.

A Tori connected mESH (TESH) network [2]-[6] is a hierarchical interconnection network for large-scale on-chip multicomputers. It consists of multiple basic modules (BMs) which are 2D-mesh networks and the BMs are hierarchically interconnected by a 2D-torus (*k*-ary 2-cube) to build higher level networks. Such networks with hierarchical structure assumed to be implementing in 3D-VLSI.

DOI: 10.14738/tnc.33.1293
Publication Date: 02th July, 2015
URL: http://dx.doi.org/10.14738/tnc.33.1293

On the other hand, restricted use of physical links between silicon planes reduced performance of the TESH network. We have proposed a deterministic, dimension-order routing algorithm[7]-[10] for the TESH network and have shown that Level-3 TESH networks have higher performance than a *k*-ary 2-cube. The minimum number of virtual channels[11] per link in dimension order routing has been proven to be two[7].

An adaptive routing algorithm can also be implemented using additional virtual channels. Based on adaptive routing algorithms of *k*-ary *n*-cube[12]-[16], we have proposed three adaptive routing algorithms for TESH[17]-[20]. In [17], three adaptive routing algorithms were proposed, and those algorithms were implemented by HDL (Hardware Description Language)[18]-[20]. By those studies, time delay and hardware cost for implement different adaptive routing algorithm were evaluated. It was shown that the time delay of adaptive routing algorithm were almost same as that of deterministic dimension order routing.

In our previous studies, we have evaluated various traffic patterns for the performance evaluation using dimension order routing. In [20] and [21], we have evaluated the hotspot and two types of non-uniform traffic patterns of *Bit Permutation and Communication* (BPC) traffic patterns. The main objective of this paper is evaluate the dynamic communication performance of a TESH network under different non-uniform traffic patterns using our previously proposed adaptive routing algorithms. In addition to the hotspot and two types of BPC traffic patterns (perfect shuffle and complement), we consider the local traffic patterns to show the suitability of our proposed adaptive routings on a TESH network.

The remainder of the paper is organized as follows. We briefly describe the basic structure of the TESH network and dimension order routing algorithm on it in Section 2 and 3, respectively. Different adaptive routing algorithms and their time delay and hardware implementation is discussed in Section 4. The dynamic communication performance of the TESH network using these adaptive routing algorithms under the various traffic patterns is discussed in Section 5. Finally, Section 6 concludes this study.

2 Structure of the TESH network

The Tori-connected mESH (TESH) Network is a hierarchical interconnection network consisting of Basic Modules (BM) that are hierarchically interconnected to form a higher level network. The BM of the TESH network is a 2D-mesh network of size $2^m \times 2^m$. In this paper, unless specified otherwise, BM refers to a Level-1 network. Successively higher level networks are built by recursively interconnecting immediately lower level subnetworks in a 2D-torus network. A higher-level network is built using immediate lower level networks as subnet modules as a 2D-torus network of size $2^m \times 2^m$[2]. Here *m* is a positive integer and in this paper, we have considered *m*=2 i.e., 4×4 2D-mesh as BMs and 4×4 2D-torus (*k*-ary 2-cube) as higher level networks as shown in Figure 1.

A $2^m \times 2^m$ BM has 2^{m+2} free ports at the contours for higher level interconnection. For each higher level interconnection, a BM uses $4 \times 2^q = 2^{q+2}$ of its free links, 2×2^q free links for vertical interconnections and 2×2^q free links for horizontal interconnections. Here, $q \in \{0,1,\cdots,m\}$ is the inter-level connectivity. *q*=0 leads to minimal inter-level connectivity, while *q*=*m* leads to maximum inter-level connectivity. Considering the size of the basic module *m*, level of hierarchy *n*, and inter-level connectivity *q*, we can define the TESH network as TESH(*m*,*L*,*q*) networks. Since we have considered *m* = 2, a Level-2 network, can be formed by interconnecting $2^{2\times2}$=16 BMs. Similarly, a Level-3 network can be formed by interconnecting 1 Level-2 subnetworks, and so on. Each BM is

connected to its logically adjacent BMs. To avoid clutter, the wraparound links of the BMs are not shown in Figure 1. In the rest of this paper we consider m=2, therefore, we focus on a class of TESH(2,L,q) networks.

The highest level network which can be built from $2^m \times 2^m$ BM is $L_{\max} = 2^{m-q} + 1$. With *m*=2 and *q*=0, $L_{\max} = 2^{2-0} + 1 = 5$. The total number of nodes in a TESH network is $N = 2^{2mL}$. Using maximum level of hierarchy, $L_{\max} = 2^{m-q} + 1$, the maximum number of nodes which can be interconnected by a TESH(*m*,*L*,*q*) is $N = 2^{2m(2^{m-q}+1)}$. With *m*=2 a Level-2 TESH network consists of 256 nodes. Similarly a Level-3 networks consists of 4096 nodes.

Processing elements (PEs) or node in a TESH(*m*,*L*,*q*) network are addressed using base-2^m numbers as follows.

$$\begin{aligned} n &= n_{2L-1}\, n_{2L-2} \cdots n_3 n_2 n_1 n_0 \\ &= (n_{2L-1}\, n_{2L-2}) \cdots (n_3 n_2)(n_1 n_0) \end{aligned} \tag{1}$$

Here, $(n_{2i-1}\, n_{2i-2})$ is the location of a subnetwork at level *i*-1. For example, in a Level-3 TESH with *m*=2, each PE is addressed by a base-4 number $n = n_5 n_4 n_3 n_2 n_1 n_0$, where n_5 and n_4 address of a PE in the Level-3 network, n_3 and n_2 address of a PE in the Level-2 network, and n_1 and n_0 address of a PE in the BM. The numerical values shown in Figure 1 are at BM address $n_3 n_2$ of a Level-2 TESH network.

The assignment of free ports for inter-level connections for the higher level networks has been done quite carefully so as to minimize the higher level traffic through the BM. The address of a node n^1 encompasses in BM_1 is represented as $n^1 = n^1_{2L-1} n^1_{2L-2} \cdots n^1_3 n^1_2 n^1_1 n^1_0$. The address of a node n^2 encompasses in BM_2 is represented as $n^2 = n^2_{2L-1} n^2_{2L-2} \cdots n^2_3 n^2_2 n^2_1 n^2_0$. The node n^1 in BM_1 and n^2 in BM_2 are connected by a link if the following condition is satisfied.

$$\exists_i \left\{ n_i^1 = (n_i^2 \pm 1) \bmod 2^m \cap \ \forall_j (j \neq i \ \rightarrow \ n_i^1 = n_i^2) \right\} \tag{2}$$

where $i, j \geq 2$.

It is shown in Figure 1 that for a Level-2 TESH network, BM(0,0) connects with either BM(0,1) or BM(0,3) in the *x*-direction, i.e., ($n_3 = 0$ and $n_2 = 1$ or $n_2 = 3$), and with either BM(1,0) or BM(3,0) in the *y*-direction, i.e., ($n_2 = 0$ and $n_3 = 1$ or $n_3 = 3$).

This hierarchical interconnection of the TESH network has the following possible implementation.

- A BM is laid out in one VLSI chip and the BMs are connected by TSV. In this way Level-2 TESH network can be realized.
- A Level-2 TESH network is laid out in one chip and then they are connected by TSV. In this way Level-3 TESH network can be realized. In a Level-2 TESH network on a chip, the yield of the chip and fault tolerance is improved by carrying out hierarchical reconfiguration algorithm. The improvement of yielding in an array network using hierarchical reconfiguration algorithm is depicted in [22].

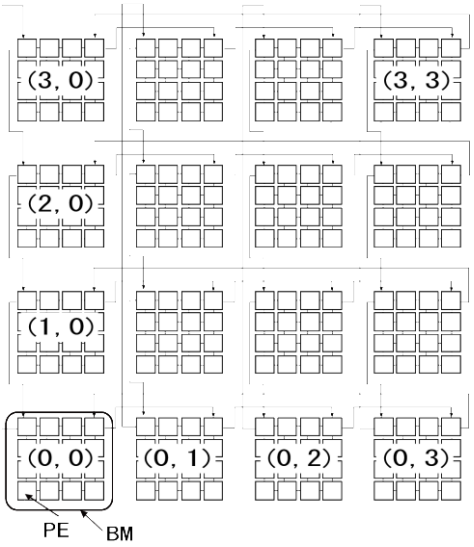


Figure 1: Hierarchical interconnection of Level-2 TESH network.

3 Dimension-Order Routing

A routing algorithm determines the path a packet takes as it travels through the network from its source to destination. A deterministic, dimension-order routing for a TESH network[7] transfers packets from higher-levels to lower-levels. That is, it is first done at the highest level network; then, after the packet reaches its highest level sub-destination, routing continues within the subnetwork to the next lower level sub-destination. This process is repeated until the packet arrives at its final destination. Packets passing through inter-BM links are forwarded from a vertical link to a horizontal link at the same level. When they arrive at the destination BM, they are transferred to the destination PE. The deterministic, dimension-order routing of Level-*L* TESH networks can generally be classified into the following three phases [7].

Phase 1: Intra-BM transfer path from source node to the outlet PE of the BM.

(PEs which hold $n_1 =$ 0,3 or $n_0 =$ 0,3)

Phase 2: Higher level transfer path.

Phase 3: Intra-BM transfer path from the outlet of the inter-BM transfer path to the destination PE.

Phase 2 is divided into the following sub-phases:

sub-phase 2.*i*.1: Intra-BM transfer to the outlet PE of Level (*L*-*i*) through the *y*-link/vertical link.

sub-phase 2.*i*.2: Inter-BM transfer of Level (*L*-*i*) through the *y*-link/vertical link.

sub-phase 2.*i*.3: Intra-BM transfer to the outlet PE of Level (*L*-*i*) through the *x*-link/horizontal link.

sub-phase 2.*i*.4: Inter-BM transfer of Level (*L*-*i*) through the *x*-link/horizontal link.

Here, $0 \leq i \leq L-2$.

We have considered the dimension order routing algorithm for the TESH network. We use the following strategy: at each level, vertical routing is performed first. Once the packet reaches the correct row, then horizontal routing is performed. Routing in the TESH network is strictly defined by the source node address and the destination node address. Let a source node address be $s = (s_{2L-1}\ s_{2L-2}) \cdots (s_3\ s_2)\ (s_1\ s_0)$ and a destination node address be

$d = (d_{2L-1}\ d_{2L-2}) \cdots (d_3\ d_2)\ (d_1\ d_0)$. The dimension-order of the TESH network is represented by R_1. Figure 2 shows the routing algorithm R_1 for the TESH network. The function *get_group_number* is the function to get group number. Arguments of this function are source PE address *s* destination PE address *d*, and direction. The function $\text{outlet}_x(g, l, d\delta)$ and $\text{outlet}_y(g, l, d\delta)$ are the function to get the value n_0 of *x* coordinate and n_1 of *y* coordinate of a PE *n* that has an inter-BM link. Variables $g, l, d\delta$ are group g $(1 \le g \le 2^q)$, level l $(1 \le l \le L)$, dimension d $(d \in \{vertical, horizontal\})$, and direction δ $(\delta \in \{+, -\})$, respectively[7].

```
/*Routing Algorithm for a Level-L TESH:*/

Routing(s, d)
s[2L]; /* source */
d[2L]; /* destination */
{

  group = get_group_number(s,d);


  for(i = 2L-1; i > 2; i--){

    if((d[i]-c[i]+2^m) mod 2^m <= (2^m)/2) dir = PLUS;
    else dir = MINUS;

    while(d[i] != c[i]){

      if(i is even number){
 outlet[0] = outlet_x(group,i/2+1,H,dir);
 outlet[1] = outlet_y(group,i/2+1,H,dir);}
      if(i is odd number){
 outlet[0] = outlet_x(group,i/2+1,V,dir);
 outlet[1] = outlet_y(group,i/2+1,V,dir);}
      if(outlet_node_x != c[0] or outlet_node_x != c[1])
        BM_routing(c, outlet);

      send_packet(dir);

  }

 }

  BM_routing(c, outlet);

}


BM_routing(c, outlet)
c[2];      /* current channel */
outlet[2]; /* outlet node */
{

  while(c[1] != outlet[1]){
    if(outlet[1] > c[1]) send_packet(UPPER);
    if(outlet[1] < c[1]) send_packet(LOWER);
 }
  while(c[0] != outlet[0]){
    if(outlet[0] > c[0]) send_packet(RIGHT);
    if(outlet[0] < c[0]) send_packet(LEFT);
 }

}
```

Figure 2: Routing algorithm of a TESH network.

4 Adaptive Routing Algorithm

Adaptive routing algorithms for TESH networks are classified into two groups: local and global algorithms. Local algorithms are defined as adaptive routing algorithms that run in one phase and global algorithms are defined as algorithms for which the order of phases can be changed.

In this section, we introduce two local adaptive routing algorithms called as channel select (CS) and link select (LS); and one global adaptive routing algorithm called dynamic dimension reversal (DDR)[17].

The deadlock in a k-ary n-cube network can be avoided using 2 virtual channels using following two conditions [14].

- Condition 1: Initially, first virtual channel (Channel-L) is used.
- Condition 2: Then the packet move to the second virtual channel (Channel-H) if the wraparound links is used for routing.

Local algorithms for TESH network are applied in sub-phases 2.*i*.2 or 2.*i*.4 in section 3. Because a ring network is formed using 4 outlet PEs (*m*=2) and inter-BM links. Local adaptive routing algorithms can be applied in this ring of TESH network. To discuss local adaptive routing algorithms, we allocate a local PE address to each of those four PEs. Let n_{local} be the local PE addresses of a ring network in the TESH. Then, n_{local} are addressed as follows:

$$n_{\text{local}} = \begin{cases} n_{2l-1}, & \text{Level} - l \text{ vertical link} \\ n_{2l-2}, & \text{Level} - l \text{ horizontal link.} \end{cases} \quad (3)$$

where n_{2l-1} and n_{2l-2} are the PE address defined in section ref{addrnd}. Below, we discuss two local algorithms for a 4-PE ring network in TESH by using n_{local}.

Since the higher-level links of TESH have *k*-ary *n*-cube network, adaptive routings of *k*-ary *n*-cube can be applied to TESH. Dynamic dimension reversal routing (DDR)[14] is proposed as adaptive routing algorithms of *k*-ary *n*-cube network. This algorithm has a lot of choice of the path and needs a few additional virtual channels. The DDR routing can also be applied to TESH network. However, unlike conventional *k*-ary *n*-cube network, the higher-level links are located in different PE in the TESH network. This is why, the choice of routing path in the TESH network is limited in comparison with *k*-ary *n*-cube network.

4.1 Channel Select (CS) Algorithm

To avoid deadlock in a ring network, two virtual channels (Channel-L and Channel-H) are needed in each direction. The CS algorithm is an adaptive routing algorithm that can use those channels freely. When wraparound channels are not used in routing, for example in the routing from PE($n_{\text{local}} = 0$) to PE($n_{\text{local}} = 2$), only Channel-L is used. In this case, because Channel-H is not used in dimension-order routing, it is possible to move from Channel-L to Channel-H or use Channel-H initially. When the routing is terminated at the output PE of a wraparound channel such as the routing from PE($n_{\text{local}} = 2$) to PE($n_{\text{local}} = 0$), only Channel-L is required. Therefore, it is possible to move from Channel-L to Channel-H or use Channel-H initially.

For dimension-order routing in a 4-PE ring network, the conditions for using only Channel-L are as follows:

- Wraparound channels are not used in routing.
- The routing is terminated at the output PE of a wraparound channel.

When the above conditions hold, the virtual channels are used according to the following order:

- Either Channel-L or Channel-H is used.
- The packet moves from Channel-L to Channel-H in the routing path.

The CS algorithm is an adaptive routing algorithm that can use virtual channels effectively. When the following three conditions hold in a 4-PE bidirectional ring network is deadlock-free[17]. The routing algorithm that applies this channel-selection principle is denoted as R_2.

Condition-1: Use Channel-L initially.

Condition-2: Use Channel-H when a wrap-around link exists in the higher level network.

Condition-3: When a packet is in a Channel-L satisfies either of the following conditions, it can move to Channel-H.

- Wrap-around links are not used in routing.
- The routing will be terminated at the output PE of a wraparound link.

4.2 Link Select (LS) Algorithm

Sub-phases 2.*i*.2 and 2.*i*.4 form a ring network. If the number of hops from the source PE to the destination PE is equal in the clockwise direction and in the counter-clockwise direction, then the packet can follow either of these two directions. The distance from $\mathrm{PE}_0(n_{\mathrm{local}}=0)$to $\mathrm{PE}_2(n_{\mathrm{local}}=2)$ in a 4-PE ring network is 2 in both the clockwise and counter-clockwise direction. Packet can follow path-a in the clockwise direction or path-b in the counter-clockwise direction.

If the following equation is satisfied, a packet can select from either a clockwise or counter-clockwise direction.

$$|s-d|=\frac{2^m}{2} \tag{4}$$

where *s* and *d* denote the source and destination PE addresses, respectively. The routing algorithm that applies this link-selection principle is denoted as R_3.

The CS algorithm is used to select a virtual channel in a physical link and the LS algorithm is used to select a physical link in a network. Therefore, both the CS and LS algorithms can be applied at the same time.

4.3 Dynamic Dimension Reversal (DDR) Algorithm

The dimension-order routing strictly maintain the restriction of routing dimension in an interconnection network, such as *k*-ary *n*-cubes. In the dimension-order routing for the TESH network the order of routing phases is fixed. However, an algorithm that can break the dimension order has already been proposed[14]. In this paper, the Dimension Reversal (DR) routing algorithm is applied in the TESH network. Dimension reversal routings of *k*-ary *n*-cubes are classified into two types: Static Dimension Reversal and Dynamic Dimension Reversal. Because Dynamic Dimension Reversal routing (DDR) can use channels efficiently, we apply DDR to a TESH. We called it as global adaptive routing algorithm. The DDR algorithm can be applied individually and simultaneously with the CS and LS algorithms.

In the DDR algorithm, each packet has a DR number, which is a count of the number of times that a packet has been routed from a channel in sub-phase 2.*p* to a channel in a lower-order sub-phase 2.*q*, *q* < *p*. Here, the format of *p* and *q* are $p_1.p_0$ and $q_1.q_0$. We assume that $p_1$and q_1 are the high-order digits and p_0 and q_0 are the low-order digits when *p* and *q* are compared. DR numbers are assigned as follows:

1. All packets are initialized with a DR of 0.
2. If a a packet routes from a channel c_i of sub-phase 2.*p* to a channel c_j of sub-phase 2.*q*, then its DR is incremented.

The DDR algorithm divides the virtual channels into two classes: adaptive and deterministic. Packets originate in the adaptive channels and while they are in adaptive channels, they may be routed by adaptive routing. Whenever a packet acquires a channel, it labels the channel with its DR number. To avoid deadlock, a packet with a DR of *p* need not to wait for a channel labeled with a DR of *q* if $p \geq q$. A packet that reaches a node where all output channels are occupied by packets with equal or lower DR numbers must switch to the deterministic channels. When a packet enters the deterministic channels, it must be routed by dimension-order routing and cannot re-enter the adaptive channels.

The adaptive routing algorithm for the adaptive channel is as follows. A packet with DDR routing of a *k*-ary *n*-cube network can be routed in any direction using adaptive channels. However, since a TESH is a hierarchical network, higher-level links of a *k*-ary *n*-cube network, where each node of this *k*-ary *n*-cube is not located in the same BM. Therefore, the packet cannot be routed freely.

There are four outlet PEs in an inter-BM links in each BM as shown in Figure 1. When the packet goes through those PEs during intra-BM routing, it can select a path from the following ones:

- Path 1: Interrupt the intra-BM routing and select the inter-BM link.
- Path 2: Continue the intra-BM routing.

When the above conditions hold, the packet selects path-1 first.

An example of the DDR algorithm applied to a TESH network is shown in Figure 3. The half-tone PE is the source PE, and the solid arrow in the BM is the deterministic routing path. In this example, we assume that a packet goes through first in a Level-3 vertical link and next in a Level-3 horizontal link. In the dimension-order routing of a TESH network, a packet is forwarded to the outlet PE of a Level-3 vertical link in phase 1 routing. However, in the DDR routing as shown in Figure 3 the packet goes through the outlet PE of a Level-3 horizontal link. When the packet reaches the outlet PE, it checks whether the Level-3 horizontal link is available or not. If it is available, the packet selects Path-1 and uses the Level-3 horizontal link before going to the outlet PE of the Level-3 vertical link. If it is not available, the packet selects Path-2 and continues with the phase 1 transfer.

The routing algorithm that applies DDR is denoted as R_4. The CS, LS, and DDR algorithms applies in the different resources of a network. Thus, these algorithms can be applied simultaneously to a network.

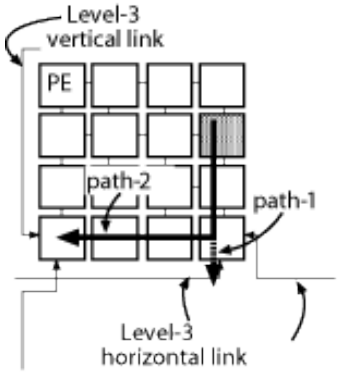


Figure 3: DDR algorithm in a TESH.

4.4 The Time Delay with Hardware Implementation

In our previous study, we have implemented the router by using VHDL language and Xilinx Project Navigator synthesis tool [18]-[20]. We have evaluated the time delay with hardware implementation using 4 virtual channels as tabulated in Table 1. Dimension order routing (DOR) is widely used in the contemporary massively parallel computers. As we have seen from Table 1, the time delay of DDR is almost same as that of DOR. Thus, we can conclude that DDR is practically implementable.

According to the clock cycle driven in [20], we evaluated the dynamic communication performance and plotted in Figure 4. The clock time in Table 1 are used for the evaluation of each routing algorithms. One cycle time is the clock time of each algorithm in Table 1. The average transfer time as a function of network throughput is portrayed in Figure 4 using uniform traffic pattern for four channels. The horizontal axis indicate network throughput, i.e., the average number of flits delivered through the network per unit time. The throughput is the number of delivered flits per PE in 1 ns, i.e., Flits / PE·ns.

As shown in Figure4, the maximum throughput of the CS and LS algorithms on a TESH network is noticeably higher than that of the dimension-order routing. In the CS algorithm, there is no influence of channel selection circuit delay. In the LS algorithm, the delay is slightly high. However, the difference is trivial. The maximum throughput using normal implementation[20] of DDR algorithm is lower than that of other algorithms. Due to complicated routing principle of DDR algorithm, its link selection circuit delay is large, which in turns make the clock cycle time of DDR algorithm long. On the other hand, the maximum throughput of parallel-implemented[20] DDR algorithm is higher than that of other algorithms.

Table 1: The Time Delay of Routing Algorithms with 4 channels (ns).

Algorithm	Cycle Time (ns)
Dimension Order	11.86
CS	11.86
LS	12.89
DDR	11.87

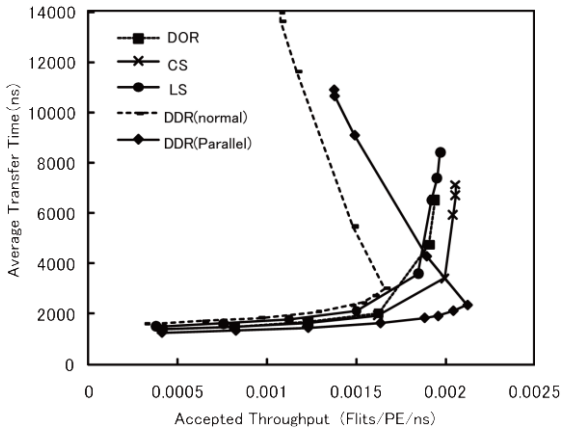


Figure 4: Comparison of dynamic communication performance of the TESH(2,3,0) network using hardware implemented router between dimension-order, CS, LS, and DDR algorithms with uniform traffic pattern: 4096 nodes, 4 VCs, and 16 flits.

5 Performance Evaluation

5.1 Simulation Environment

We have developed a wormhole routing simulator to evaluate dynamic communication performance of the TESH(2,3,0) network with 4096 PE. Dynamic communication performances are simulated for dimension-order routing algorithm, CS algorithm, LS algorithm, DDR algorithm, and combinations of them.

Extensive simulations have been carried out for the following traffic patterns.

- uniform
- hotspot
- perfect shuffle
- complement
- local communication

The dynamic communication performance of an interconnection network is characterized by message latency and network throughput. Message latency refers to the time elapsed from the instant when the first flit is injected into the network from the source to the instant when the last flit of the message is received at the destination. Average transfer time is the average value of the latency for all packets. Network throughput refers to the maximum amount of information delivered per unit of time through the network. It is the average value of the number of flits which a PE receives in each clock cycle. In the evaluation of dynamic communication performance, flocks of messages are sent in the network to compete for the output channels. Packets are transmitted by the request-probability r during T clock cycles and the number of flits which reached at destination PE and its transfer time are recorded. Then the average transfer time and throughput are calculated and plotted as average transfer time in the horizontal axis and throughput in the vertical axis. The process of performance evaluation is carried out with changing the request-probability r.
The packet size is 16 flit and flits are transmitted for 20,000 cycles, i.e., T=20000. In each clock cycle, one flit is transferred from the input buffer to the output buffer, or from output to input if the corresponding buffer in the next node is empty. Therefore, transferring data between two nodes takes 2 clock cycles. Four virtual channels per physical channel are simulated, and they are arbitrated by a round-robin algorithm. The buffer length of each channel is 2 flits. In the DDR algorithm, the number of deterministic channel and adaptive channel are two respectively. In other algorithms, a pair of channels is used for deadlock avoidance, and two pairs are used to select channels. The transfer method of the packet is wormhole routing[23].

5.2 Uniform Traffic Pattern

In a uniform traffic, destinations are chosen randomly with equal probability among the nodes in the network. The result of uniform traffic was shown in [20].

Figure 5 shows the average transfer time as a function of network throughput[20]. The horizontal axis indicates network throughput and the vertical axis indicates transfer time. Also, the number inside the figure is the request-probability r. From Figure5, the throughput of CS, LS, and DDR algorithms and those combinations are higher than DOR.

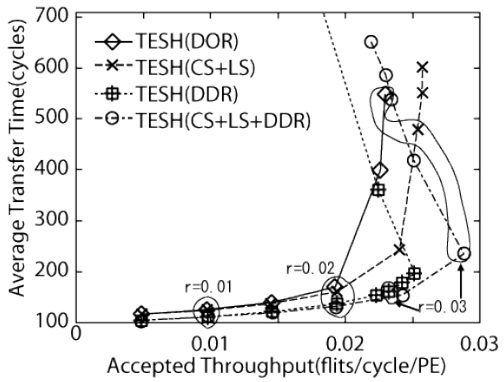


Figure 5: Comparison of dynamic communication performance of the TESH(2,3,0) network between dimension-order, CS+LS, DDR, CS+LS+DDR algorithms with uniform traffic pattern: 4096 nodes, 4 VCs, and 16 flits.

5.3 Hotspot Traffic Pattern

In a uniform traffic, destinations are chosen randomly with equal probability among the nodes in the network. The result of hotspot traffic was also shown in [20].

Figure 6 shows the average transfer time as a function of network throughput[20]. As depicted in Fig.6, the DDR algorithm has a low average transfer time in comparison with the other algorithms at zero-load like uniform traffic pattern. Also the maximum throughput of the DDR algorithm under hot-spot traffic pattern is higher than that of other algorithms. Because the choice of the inter-BM link is more than that of CS and LS algorithms. In this experiment, higher-level links of the neighborhood of destination PE are congested because hotspot packets use higher-level links intensively. Global adaptive routing algorithm such as DDR algorithm has an advantage in hot-spot traffic pattern because a lot of inter-BM links can be selected as compared with local adaptive routing. Therefore, with the hot-spot traffic pattern, the DDR algorithm yields better dynamic communication performance than that of dimension-order, LS, and CS algorithms.

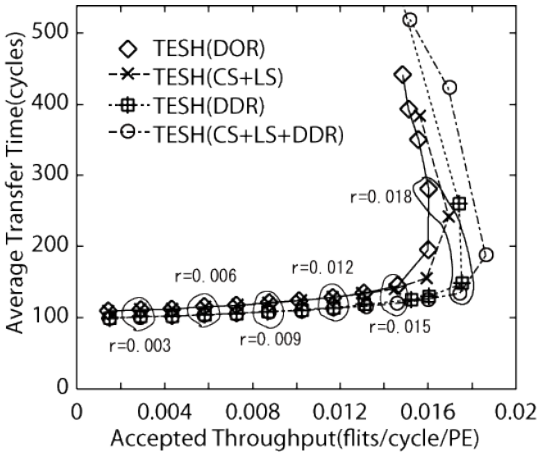


Figure 6 Comparison of dynamic communication performance of the TESH(2,3,0) network between dimension-order, CS+LS, DDR, CS+LS+DDR algorithms with hot-spot traffic pattern: 4096 nodes, 4 VCs, and 16 flits.

5.4 Bit Permutation and Communication (BPC) Traffic Pattern

Bit Permutation and Computation (BPC) [24] is a class of non-uniform traffic pattern, which are very common in scientific applications. BPC communication patterns take into account the permutations that are usually performed in parallel numerical algorithms [25][26]. These distributions achieve the maximum degree of temporal locality and are also considered as benchmarks for interconnection

networks. Among various BPC traffic patterns, in this paper, we have considered complement and perfect shuffle traffic pattern.

5.4.1 Complement Traffic Pattern

In the complement traffic pattern, the source PE $n_s = (n_{2L-1}\, n_{2L-2}) \cdots\cdots (n_3 n_2)(n_1 n_0)$ sends packet to the destination PE

$n_d = \overline{n_s} = (\overline{n_{2L-1}}\, \overline{n_{2L-2}}) \cdots\cdots (\overline{n_3}\, \overline{n_2})(\overline{n_1}\, \overline{n_0})$. In this traffic pattern, all the packets cross the bisection of the network. All communications are inter-level which creates the congestion in the inter-BM links.

Considering this congested scenario, we have evaluated by simulation the dynamic communication performance of the TESH network using DOR, LS, CS, and DDR algorithm and the result is plotted in Figure 7. From Figure 7, it is seen that dynamic communication performance of the CS and LS algorithm is almost similar to that of DOR algorithm. Due to the congestion in the middle of the network, the performance improvement by CS and LS algorithm is limited. It is also shown that the average transfer time and throughput under DDR algorithm is slightly improved than that of other algorithm.

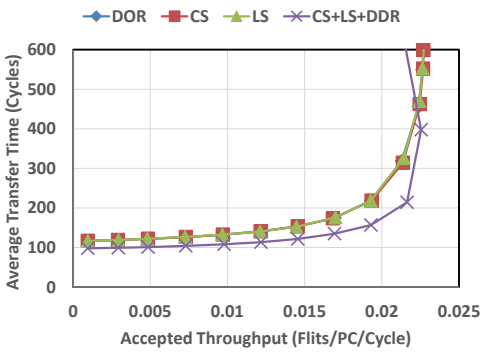


Figure 7: Comparison of dynamic communication performance of the complement traffic pattern on the DOR and adaptive routings for TESH(2,3,0) network: 4096 nodes, 4 VCs, and 16 flits.

5.4.2 Perfect Shuffle Traffic Pattern

Let the source PE address be n_s and the destination PE address be n_d. According to the perfect shuffle traffic pattern the destination PE n_d is determined as follows:

Let the source PE address be n_s and the destination PE address be n_d. According to the perfect shuffle traffic pattern the destination PE n_d is determined as follows:

$$n_d = \begin{cases} n_s \times 2 & (\ n_s < N/2) \\ (\ n_s - N/2) \times 2 + 1 & (\ n_s \geq N/2) \end{cases} \quad (5)$$

We have evaluated the dynamic communication performance of the TESH network using DOR, LS, CS, and DDR algorithm under perfect shuffle traffic pattern and the result is plotted in Figure 8. From Figure 8, it is shown that the throughput is considerably improved by DDR algorithm and slightly improved by LS algorithm. In the perfect shuffle traffic, the probability of packet reach to the destination in intra-BM is same as uniform traffic pattern. Therefore, it has the similar performance as that of uniform traffic.

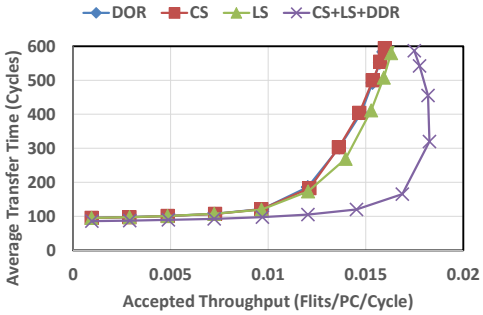


Figure 8: Comparison of dynamic communication performance of the perfect shuffle traffic pattern on the DOR and adaptive routings for TESH(2,3,0) network: 4096 nodes, 4 VCs, and 16 flits.

5.5 Local Communication Traffic Pattern

In some applications, there are a lot of communications between neighborhood nodes. To study this phenomenon in hierarchical interconnection network, we have evaluated the communication performance of a TESH network using local communication. In this traffic pattern, each node first generates a random number. If that number is less than a predefined threshold, the message will be sent to the destination PE in same BM. Otherwise, the message will be sent to any other nodes, with a uniform distribution. In this pattern, packet is sending from $\mathrm{PE}_s = (n_{s5}n_{s4})(n_{s3}n_{s2})(n_{s1}n_{s0})$ to $\mathrm{PE}_l = (n_5n_4)(n_3n_2)(n_{d1}n_{d0})$.

The local packet generation probability are assumed to be from $P_l = 0.0$ (all packets are sent to PE in other BMs) to $P_l = 1.0$ (all packets are local packet).

Figure 9 depicts the maximum throughput with respect to the local packet generation probability. Figure 10 portrays the ratio between maximum throughput of different adaptive routing algorithm and DOR ($Th_{\mathrm{Ad}}/Th_{\mathrm{DOR}}$) with respect to local packet generation probability. Here, Th_{DOR} is the maximum throughput using DOR and Th_{Ad} is the maximum throughput using adaptive routing algorithm. Thus the ratio $Th_{\mathrm{Ad}}/Th_{\mathrm{DOR}}$ is plotted in the *y*-axis and local packet generation probability is plotted in the *x*-axis.

As illustrated in these figures, the performance is improved using CS and LS algorithm when P_l is low and the performance is considerably improved using DDR algorithm when P_l is higher. Therefore, DDR is a suitable algorithm for local communication in the hierarchical interconnection network such as TESH because the performance is improved when P_l is higher.

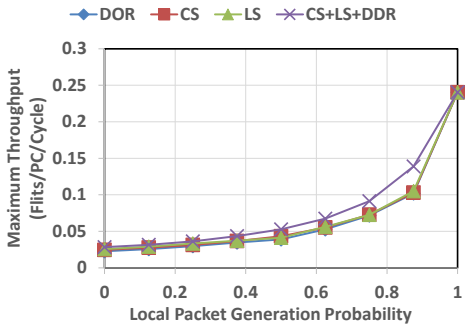


Figure 9: Comparison of maximum throughput of the local traffic pattern on the DOR and adaptive routings for TESH(2,3,0) network: 4096 nodes, 4 VCs, and 16 flits.

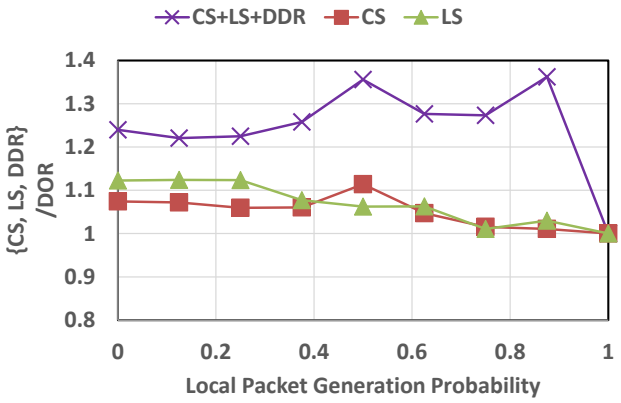


Figure 10: Comparison of maximum throughput with the DOR and adaptive routings of the local traffic pattern on the for TESH(2,3,0) network: 4096 nodes, 4 VCs, and 16 flits.

6 Conclusion

We have proposed three adaptive routing algorithms, CS, LS, DDR along with dimension-order routing with their hardware implementation for the TESH network. The proposed algorithms are simple and efficient for using the virtual channels, physical links, and direction of network to improve dynamic communication performance.

In this paper, we have evaluated the dynamic communication performance using different non-uniform traffic patterns named hotspot, complement, perfect shuffle and local communication traffic patterns. It was shown that the dynamic communication performance using DDR algorithm in a TESH network is slightly improved in the complement traffic and significant improved in the perfect shuffle traffic patterns. Also, in local communication traffic pattern, the dynamic communication performance is highly improved when inter-BM communications appear frequently.

In the application of hierarchical interconnection network, it is thought that data are laid out so that communication with neighborhood may become a lot. Therefore, DDR is suitable for the hierarchical interconnection network such as TESH.

REFERENCES

[1] W.J. Dally, Performance Analysis of *k*-ary *n*-cube Interconnection Networks, *IEEE Trans. on Computers*, vol. 39, No.6, pp.775--785, 1990.

[2] V.K. Jain, T. Ghirmai, and S. Horiguchi, TESH: A new hierarchical interconnection network for massively parallel computing, *IEICE Trans. on Inf. & Syst.*, Vol.E80-D, No.9, pp.837-846, 1997.

[3] V. K. Jain, T. Ghirmai and S. Horiguchi, Reconfiguration and Yield for TESH: A New Hierarchical Interconnection Network for 3-D Integration, *IEEE Proceedings of International Conference Wafer Scale Integration*, pp. 288-297, 1996.

[4] V.K. Jain and S. Horiguchi, VLSI Considerations for TESH: A New Hierarchical Interconnection Network for 3-D Integration, *IEEE Trans on VLSI Systems*, Vol.6, No. 3, pp. 346-353, 1998.

[5] S. Bhansali et al., 3D heterogeneous sensor system on a chip for defense and security applications, *Proceedings of the SPIE Defense and Security Symposium (DSS)*, pp.413-424, 2004.

[6] G. H. Chapman, V. K. Jain and S. Bhansali, Defect Avoidance in 3-D Heterogeneous sensor, Proceedings of the 19th IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems (DFT'04), pp.67-75, 2005.

[7] Y. Miura and S. Horiguchi, A Deadlock-Free Routing for Hierarchical Interconnection Network: TESH, *Proc. of the Fourth International Conference on High Performance Computing in Asia-Pacific Region*, pp.128-133, 2000.

[8] M.M. Hafizur Rahman, Y.Inoguchi, Y.Sato, Y.Miura and S.Horiguchi, On Hot-Spot Traffic Pattern of TESH Network, *11th International Conference on Computer and Information Technology(ICCIT 2008)*, 2008.12.

[9] M.M. Hafizur Rahman, Y.Inoguchi, Y.Sato, Y.Miura and S.Horiguchi, Dynamic Communication Performance of a TESH Network under the Nonuniform Traffic Patterns, *11th International Conference on Computer and Information Technology(ICCIT 2008)*, 2008.12.

[10] M.M. Hafizur Rahman, Y.Inoguchi, Y.Sato, Y.Miura, S.Horiguchi, Dynamic Communication Performance of the TESH Network under Nonuniform Traffic, *Journal of Networks*, Vol.4, No.10, pp.941-951, 2009.12.

[11] W.J. Dally, Virtual-Channel Flow Control, *IEEE Trans on Parallel and Destributed Systems*, Vol.3, No.2, pp.194-205, 1992.

[12] C. S. Yang and Y. M. Tsai, Adaptive Routing in k-ary n-cube Multicomputers, *Proc. of ICPADS '96*, pp.404-411, 1996.

[13] W.J. Dally and C.L.Seitz, Deadlock-Free Message Routing in Multiprocessor inter-connection Networks, *IEEE Trans. on Computers*, Vol.C-36, No.5, pp.547-553, 1987.

[14] W.J. Dally and H. Aoki, Deadlock-Free Adaptive Routing in Multicomputer Networks Using Virtual Channels, *IEEE Trans. on Parallel and Distributed Systems*, Vol. 4, No. 4, pp.466-475, 1993.

[15] C.J. Glass and L. M. Ni, Maximally Fully Adaptive Routing in 2D Meshes, *ISCA92*, pp.278-287, 1992.

[16] J. Duato, A New Theory of Deadlock-Free Adaptive Routing in Wormhole Networks, *IEEE Trans. on Parallel and Distributed Systems*, Vol.4, No.12, pp.1320-1331, 1993.

[17] Y. Miura and S. Horiguchi, An Adaptive Routing for Hierarchical Interconnection Network TESH, *Proc. of the Third International Conference on Parallel And Distributed Computing, Applications and Technologies*, pp. 335-342, 2002.

[18] Y. Miura, M. Kaneko and S. Horiguchi, Examination of Hardware Implementation on Adaptive Routing for Hierarchical Interconnection Network TESH, *Proc. of International Workshop on High Performance and Highly Survivable Routers and Networks (HPSRN 2008)*, 2008.

[19] Y.Miura, M.Kaneko, S.Watanabe, Adaptive Routing Algorithms and Implementation for Interconnection Network TESH for Parallel Processing, *The 35th IEEE Conference on Local Computer Networks (LCN)*，2010.10.

[20] Y.Miura, M.Kaneko, M.M.Hafizur Rahman and S.Watanabe, Adaptive Routing Algorithms and Implementation for TESH Network, *Communications and Network (CN)*, Vol.5, No.1, pp.34-49, 2013.02.

[21] Y. Miura, S. Watanabe, and M.M. Hafizur Rahman, The Communication Performance of Adaptive Routing for Hierarchical Interconnection Network for 3D VLSI, Proc. of 2015 International Conference on Information, Computer and Communication Engineering (ICC 2015) (Accepted).

[22] N.Tsuda, Hierarchical redundancy for array-structure WSIs, *Journal of Systems and Computers in Japan*, Vol.24, No.7, pp.13--30, 1993.

[23] L. M. Ni and P. K. McKinley, A Survey of Wormhole Routing Techniques in Direct Networks, *Computer*, Vol.26, No.2, pp.62-76, 1993.

[24] M. Grammatikakis, D.F. Hsu, M. Kratzel and J.F. Sibeyn, Packet routing in fixed connection networks: a survey, *Journal of Parallel and Distributed Computing*, Vol. 54, No. 2, pp.77–132, 1998.

[25] Andrew A. Chien and Jae H. Kim, Planer-Adaptive Routing:Low-cost Adaptive Networks for Multiprocessors, *Journal of the ACM*, Vol.42, No.1, pp.91–123, 1995.

[26] P.R. Miller, Efficient Communications for Fine-Grain Distributed Computers, *Ph.D. Dissertation, Southampton University*, U.K., 1991.