INTERNATIONAL JOURNAL OF INFORMATION TECHNOLOGY AND APPLICATIONS (IJITA)

Volume 3, Issue 1, Dec (2015), ISSN 0976-8661 (PRINT)

Published By:
Department of Computer Science and Engineering
Institute of Engineering and Technology
Affiliated to Rajasthan Technical University (RTU), Kota.

INTERNATIONAL JOURNAL OF INFORMATION TECHNOLOGY & APPLICATIONS (IJITA)

July - December 2015 **Volume -3, Issue - 1** **ISSN (Print): 0976-8661**

Institute of Engineering & Technology,

North Extension, MIA, Alwar-301030(Rajasthan)

Website: www.ietalwar.com

INTERNATIONAL JOURNAL OF INFORMATION TECHNOLOGY & APPLICATIONS (IJITA)

EDITORIAL

We are profoundly privileged to bring before you the efforts of few genius minds in the form of **"INTERNATIONAL JOURNAL OF INFORMATION TECHNOLOGY & APPLICATIONS (IJITA)".** Its aim is to encourage and make aware scholars, students, engineers & faculty towards the scientific & technical attitude for better living in science and technology world.

If technology is adopted in education, it will make better future. Also high productivity, beneficial education and long-term advantages are expected.

America has attempted to develop their education and thereby the Goals 2000 which guides education was established. There are some information tools such as computers and communication networks known as Super highway information.

Education institutions regardless of its size are required to provide a gateway to the information superhighway. Also because it makes home closer to schools and libraries, community leaders have to ensure that all children have the opportunity to access it. Especially, for children who are poor or disabled and isolated it is very valuable. Moreover, it makes the nation get higher production and lower benefit Payment.

Adoption of technology in education must be seen as an investment rather than as an expense. Schools need a plan which aims at high achievement and addresses the needs of students. Moreover cutting-edge technology should be given for schools in poor areas. Finally, as the changes required in implementing technology may make a long time, schools should not be rigid in their requirements.

The foundation blocks of research are to do the right thing, at right time, in right way anticipate requirement, to develop resources and then to recognize no impediments and thence to master circumstances.

We congratulate and wish good luck to the researchers for their contribution. These efforts will act as a lighthouse to the current & future generation to success in the field of science & technology.

Prof. (Dr.) Anil Kumar Sharma

Chief Editor

INTERNATIONAL JOURNAL OF INFORMATION TECHNOLOGY & APPLICATIONS (IJITA)

MESSAGE

My dream, hard work & vision of imparting best quality Engineering Education in Rajasthan comparable with the best in the world has born fruits by getting AICTE - NBA Accreditation of Institute of Engineering & Technology College for all Branches of Engineering.

Institute of Engineering & Technology, Alwar aims at imparting sound technical knowledge to engineering, Management graduates and Postgraduates in accordance with the Industrial Standards. This helps the Professional Graduates and Postgraduates to develop Managerial skills.

The past ten years of journey of IET, Alwar, starting since 1998 is a journey of hard work, dedication, self discipline and motivation as I have fulfilled my ambition of establishing IET-Alwar, as an Engineering Institute par excellence & equipped with State-of-art Laboratories, Computer and IT departments, excellent building infrastructure with lush green landscaping and well qualified, experienced & committed team of faculty members.

We give more emphasis on programs with high demands and those, which will help students to face National and International challenges in professional career.

I am confident enough about IET's growth as one of the best educational group in the country especially in the field of Technical Education.

However, the journey of knowledge never ends. Each student who take admission in IET, Alwar has to follow the following "Guru Mantra" for his whole life:

"Hard work has no substitute; sooner or later only hard work gives best Reward"

Dr. V. K. AGARWAL- MBBS,MD, MBA
Chancellor SunRise University &
Chairman, IET Group of Institutions, Alwar

INTERNATIONAL JOURNAL OF INFORMATION TECHNOLOGY & APPLICATIONS (IJITA)

MESSAGE

IET, Alwar is the First Private Engineering College of Rajasthan and now the first college of the state to be fully accredited by NBA.This is the hard work of the entire team, comprising of management & faculty members.

Technical Challenges & expectations of the market need sound Technocrats and managers. We aim to provide quality Education to the students, which help them to face the world with confidence. We also aim to provide appropriate and healthy environment to faculty and students so that the focus is entirely on studies and technological growth.

Separate Girls and Boys hostels are located inside the campus. High priority is given to the safety and security of girl students. We aim to provide a home away from home to each student.

I am confident that IET, Alwar will soon reach a degree of excellence due to the Vision of the management, dedicated faculty and hard working students.

I wish a very prosperous career graph for the students each one must

"Create a concrete action plan and dedicate yourself to achieve your Goal / Dream"

Dr. MANJU AGARWAL - MBBS, MBA
Executive Director,
IET Group of Institutions, Alwar

INTERNATIONAL JOURNAL OF INFORMATION TECHNOLOGY & APPLICATIONS (IJITA)

July - December 2015 Volume -3, Issue - 1 ISSN (Print): 0976-8661

Contents

About IET

Institute of Engineering & Technology, Alwar the First self-financed college of Rajasthan and promoted by the A.I.S.A.E.R. (All India Society for Advance Education & Research), New Delhi was established in the Year 1998 at Alwar. The Institute was given NOC and approval by the A.I.C.T.E. on 07 July, 1998. Institute obtained affiliation from the University of Rajasthan, Jaipur on 04 August, 1998. The single institute venture over the years has grown up and become a Group of Academic Institutions that include 2 Engineering Institutes, a Pharmacy, Biotechnology & a Management College by now.

The Engineering colleges managed by this group are providing Technical Education in 7 Engineering Branches at Under Graduate Level and 5 Branches at Post Graduate Level, a rare combination present in education in private sector in whole of North India. The Biotechnology stream is available at UG and PG in Biotechnology Institute. Pharmacy College is catering to B. Pharma. Students and the Management studies are delivering quality education for various UG and PG management courses. The IET Group is managed by a group of visionary professionals lead by its **Chairman, Dr. V. K. Agarwal (MBBS, MD, MBA**) with a vision to fulfill a finest Educational Standards in Northern India particularly in Rajasthan. Dr. V. K. Agarwal as Chairman of the group is supported by **Executive Director, Dr. Manju Agarwal (MBBS, MBA).**

The IET Group's requirement to have highly capable & entrepreneurial professionals at the helm of the institute created a true success as a result of extra creativity, innovativeness and dynamism to take-up challenges.IET Group has the privilege of becoming The First Private Engineering College of Rajasthan Established in 1998.

Approx. 2500 Students are presently studying in the IET from various part of India. Excellent Placement Records, almost 75% students placed through Campuses.

A Comparative Study of Futuristic Wireless Data Transmission Technique *Li-Fi* with Existing *Wi-Fi*

Dr. Birendra Rai[1], Harish Dadhich[2],Vivek Rai[3]

[1]Professor & Principal, [2]Associate Professor,[3]M.Tech Scholar

[1,2]Vyas College of Engineering & Technology, Jodhpur, Rajasthan,

[3]Department of CSE MBM Engineering College JNV Univ, Jodhpur

Abstract

In the present scenario, the existing wireless communication technology is anticipated lack of adequate radio frequency bandwidth to meet the growing demand of multimedia data communication and internet access. Though the existing wireless data transmission techniques Wi-Fi and cloud computing are constantly expanding but these techniques are suffering from the reliable signal transmission with greater speed and high security as they are open to hacker due to its penetrating capability through walls easily. To overcome these problems, Li-Fi (Light Fidelity) a futuristic wireless data transmission technique in which the visible light spectrum instead of radio frequencies are used that enables high-speed wireless multimedia data communication and internet access. The working principle of Li-Fi is based on visible light communication (VLC) in which the light emitting diodes (LED_s) are used as a carrier signal to transmit the data wirelessly instead of traditional radio frequency as in Wi-Fi. Pure Li-Fi provides ever-present high-speed wireless access that offers substantially greater security, safety and data densities than Wi-Fi along with inherent properties that eliminate unwanted external network interruption. Li-Fi provides the better bandwidth, efficiency, availability and security than the Wi-Fi communication. Due to these advantages, in future Li-Fi data transmission technique will be more useful to all the sectors. In this paper we cover the comparative study of existing and futuristic wireless data transmission techniques Wi-Fi (Wireless Fidelity) and Li-Fi (Light Fidelity) respectively.

Keywords: Li-Fi, Wi-Fi, Radio waves, VLC (Visible Light Communication), LED (Light Emitting Diode), Bandwidth

1. Introduction

Today the computer communication and internet access Wi-Fi technology has acquired a pivotal role due to its various benefits but its excessive usage causes many challenges such as capacity, availability, efficiency and security. To overcome these challenges Li-Fi a wireless data transmission technique was introduced by German physicist Herald Haas from University of Edinburgh, UK [4].

In October 2011, a number of companies and industries formed the Li-Fi Consortium to promote high-speed optical wireless system sand to enhance the limited bandwidth available for radio wave based wireless spectrum. The consortium believes it is possible to achieve more than 10 Gbps speed using the Li-Fi which is also known as optical wireless technique. In this technique the communication is done by transmission of data through illumination using LED light bulb that varies in intensity faster than the human eye can follow [3].

Li-Fi is an advanced version of Wi-Fi or we may say it is an optical version of Wi-Fi in which when the LED switched on digital 1 and when off digital 0 is transmitted respectively. The transceiver in Li-Fi are fitted LED lamps that can be switched on and off very quickly and can glow a room as well as transmit and receive information [4].

2. Wireless Data Transmission Techniques

The Wireless Data Transmission Techniques has become fundamental to our life. We use it in our everyday life, in our

private life and business life. It has become a utility like electricity & water. Currently Wi-Fi uses radio waves for data communication

2.1 Basic Issues of wireless Data Transmission in radio waves

The basic issues of data transmission in radio waves are as follows:

(i) Capacity: The transmission of wireless data through radio waves has a limited range. The radio waves are scar and expensive and further with the advent of the generation technology such as 2.5G, 3G, 4G and so on we are running out of spectrum.

(ii) Efficiency: There are almost 1.4 million cellular radio base stations which consume massive amount of energy. Most of this energy is not use for transmission but for cooling down the base stations thereby limiting the efficiency of such a base station by 5% and that has a big problem.

(iii) Availability: Availability of radio waves causes another agony as because we have to switch off our mobiles in aeroplanes and not advisable to use at places like petrochemical plants as well as petrol

pumps.

(iv) Security: The transmission of wireless data through radio waves is not secure since it penetrates through walls and can be easily intercepted. If someone has a knowledge and bad intentions than he may misuse it

2.2 Data Transmission through Li-Fi using VLC

Since it does not depends on radio wave so it can be used easily in the places where Bluetooth, infrared, WIFI and Internet are banned. In Li-Fi VLC is a data communication medium which uses visible light between 400 THz (780 nm) and 800 THz (375 nm) as optical carrier for data transmission and illumination as shown in figure 1.

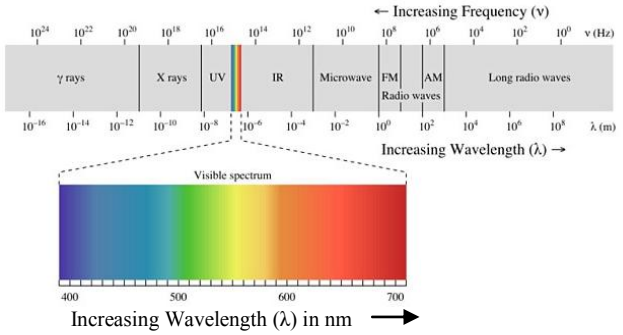


Fig.1: Li-Fi Frequency

3. Why Use Visible Light Communication (VLC)

The other spectrums such as gamma rays, x-rays and ultra-violet rays cannot be used for data transmission as they can be dangerous and risky for human beings. They are not safe from health point of view. Infrared due to eye safety regulation may be used with low power.

Compared to other spectrum visible light spectrum not used so far and it is safe to use and having larger bandwidth. On the other hand, the visible light is everywhere, and also has a wide spectrum as shown in fig

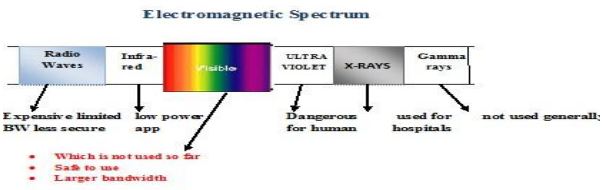


Fig. 2: Electromagnetic Spectrum

4. Working Principle of Li-Fi

In Li-Fi technology there is a light source at one end like an LED and a photo detector on the other end as soon as LED starts glowing, photo detector on the other end will detect light and get a binary1 otherwise binary 0. VLC (visible light communication) is a data communication medium, which uses visible light as optical carrier for data transmission and illumination. It uses fast pulses of light to transmit information wirelessly. The main components of Li-Fi systems are as follows:

(i) Lamp driver
(ii) Light Emitter
(iii) Photo Detector

As shown in figure 3, a internet connection is connected to the lamp driver, a switch connected with lamp driver and LED lamp also connected this lamp driver through fiber optics cable. A receiving device called photo detector is used for receiving the signals. The processing of signal has been performed after receiving the signal, this device is connected with PC or Laptop's LAN port. On one end all the data on the internet will be streamed to a lamp driver when the LED is switched on the microchip converts the digital data in form of light [6].

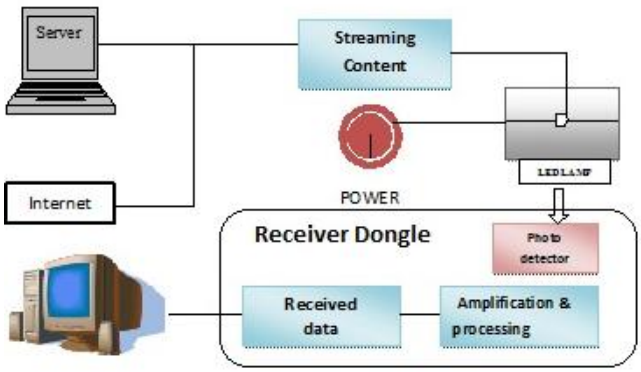


Fig.3: Working of Li-Fi

The light sensitive device photo detector receives the signal and converts it into original data signals. This method of using rapid pulses of light to transmit data wirelessly is known as, Visible Light Communication. To obtain the higher data rate data number of slightly different colors LEDs are used. Standard LED light bulbs are controlled by a driver that turns the LED on and off or dims and brighten it with Li-Fi enabled LED light bulbs, the driver is used to transmit encoded data by controlling the LED light an optical sensor is used to receive the data, which is then decoded the receiver has optics, and is fast enough to see the light dimming and brightening, smart enough to decode the Li-Fi data, and then deliver it to the attached device such as a laptop computer, a receiver dongle converts tiny charges in amplitude into an electrical signal which is then converted back into a data stream and transmitted to a device.

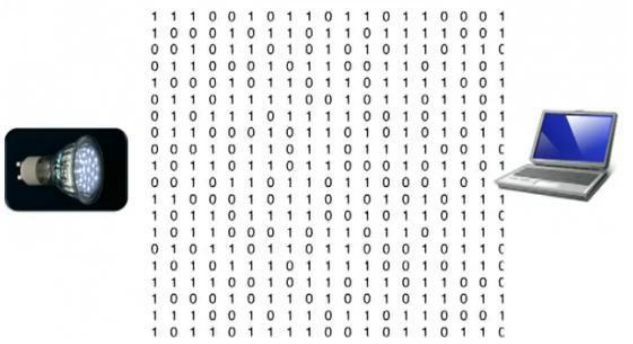


Fig.4: Li-Fi Data Transmission

It is structured according to communication Protocols set forth by the IEEE 802 workgroup. The proposed plan is to establish a wireless network using visible light.

5. Comparison between Wi-Fi & Li-Fi

Wi-Fi works well for general wireless coverage within buildings and Li-Fi is ideal for high density wireless data coverage inside a confined area or room and for relieving radio interference issues. The four major issues (capacity, efficiency, availability and security) which the current wireless system faces are easily handled by Li-Fi technology.
Comparison of existing and futuristic wireless technologies in respect of speed of data transmission and data density is depicted in the table 1

Table 1: Comparison of Wireless Technology

Wireless Technology					
Existing			**Futuristic**		
Transmission Technique	**Speed**	**Data Density**	**Transmission Technique**	**Speed**	**Data Density**
Wi-Fi IEEE 802.11n	150 Mbps	*	Wi Gig (Wireless Gigabit Alliance)	2 Gbps	**
Bluetooth	3 Mbps	**	Giga-IR	1 Gbps	***
IrDA (Infrared Data Association)	4 Mbps	***	Li-Fi	>1 Gbps	****

The comparison between existing Wi-Fi and futuristic Li-Fi wireless data transmission techniques has been shown in table 2

Table 2: Comparison between Wi-Fi and Li-Fi

S.No	**Parameters**	**Wireless Technologies**	
		Wi-Fi (Wireless Fidelity)	**Li-Fi (Light Fidelity)**
1	Speed for data transfer	Data Transfer speed (150 Mbps)	Faster transfer speed (>1 Gbps)
2	Medium through which data transfers occurs	Used Radio spectrum	Used Light as a carrier
3	Spectrum Range	Radio frequency spectrum range is less than visible light spectrum.	Visible light spectrum has 10,000 time broad spectrum in comparison to radio frequency
4	Cost	Expensive in comparison to Li-Fi because its uses radio spectrum	Cheaper than Wi-Fi because free band does not need license and it uses light.
5	Network topology	Point to point	Point to point
6	Operating frequency	2.4 GHz	Hundreds of Tera Hz

6. Advantages of Li-Fi

Since Li-Fi does not depend upon radio wave, thus it can be easily deployed in those places where Bluetooth, infrared, Wi-Fi and internet are banned. Some of the advantages of Li-Fi over other kinds of wireless data communication techniques using radio waves are as follows:

(i) Capacity: Visible light spectrum is 10000 times wider bandwidth than the radio wave bandwidth. It is predicted that will we run out of the RF spectrum by 2020.

(ii) Efficiency: Data transmission using Li-Fi is very cheap.
LED lights consume less energy and are highly efficient.

(iii) Availability: Availability is not an issue as light sources are present everywhere. There are billions of light bulbs worldwide; they just need to be replaced with LEDs for proper transmission of data.

(iv) Security: Light waves do not penetrate through walls.
So, they can‘t be intercepted and misused, thus security is higher in using Li-Fi.

(v) Transmission of data*:* Wi-Fi transmits data serially and Li-Fi transmits thousands of data streams parallely thus offering higher speed.

(vi) Infrastructure: It already exists and uses inexpensive devices mostly powered by LED. Thus, it is cost effective in comparison to the base stations of wireless data transmission technique using radio wave.

7. Applications of Li-Fi

Applications of Li-Fi can be extended in many area where the Wi-Fi technology either suffers in its presence or banned due to interfere with the radio waves such as medical technologies, power plants, aircraft flights and various other areas. Some of the future applications of Li-Fi are as follows:

(i) Intelligent Transport System: LED equipped headlight and backlights, where the cars can talk to each other and react faster when they are Li-Fi enabled. Traffic lights and street lights can talk to each other and also to the cars which can indeed reduce the number of accidents.

(ii) Underwater Awesomeness: The RF cannot penetrate in the water while the visible light can. Divers can use their torches enabled with Li-Fi technology to communicate with each other. The submarines can also transmit and receive information from the ships that are above it through transmission and reception of light.

(iii) Indoor Navigation: Li-Fi can be used to navigate through any hospital or office building that has Li-Fi enabled LED lighting through the user's smart phones.

(iv) Oil and gas wells: Testing and maintaining of gas wells can be performed with greater ease and efficiency. This can be obtained by placing the Li-Fi transmitter at the bottom of the well and the receiver at the surface, for real-time continuous monitoring.

(v) Intrinsically safe environments: This can be used in petroleum and chemical industries and other environments where the usage of radio waves or other transmission frequencies can be hazardous.

(vi) Boon for Hospitals: Operating rooms in hospitals do not allow Wi-Fi over radiation concerns and also there is lack of dedicated spectrum. Wi-Fi is in place in many hospitals but interference from cell phones and computers can block signals from the monitoring equipment. Li-Fi solves both problems. Lights are not only allowed in operating rooms but tend to be the most glaring fixtures in the room. It can also be used for advanced medical instruments.

(vii) Enjoy your Flight: The switching off mobile phones is the primary instruction of flights globally during take-off and landing. It is due to the electromagnetic interference caused to the aircraft systems by the radio waves emitted from mobile phones thus hindering our online operations. Li-Fi provides a solution to these problems as it can use the light present in the aircraft lobby for data transmission.

(Viii) Education System: With the advancement of science the latest technique will be Li-Fi for wireless data communication for the fastest speed internet access service. It will lead to the replacement of Wi-Fi at institutions and at companies so that all the people can make use of Li-Fi with same speed intended in a particular area.

8. Conclusion

The concept of Li- Fi is attracting a lot of eye-balls because it offers a genuine and very efficient alternative to radio based wireless. It also supports green environment, as it uses Visible Light Communication for transmission of data, which is harmless and available everywhere. The shortage of radio-frequency bandwidth and boot out the disadvantages of Wi-Fi. It has a bright chance to replace the traditional Wi-Fi because as an ever increasing population is using wireless internet, the radiowaves are becoming increasingly clogged, making it more and more difficult to get a reliable, high- speed signal.

Thus if this technology is put into the practical use, every LED bulb can be used as a Li-Fi hotspot for transmitting and receiving wireless data. Li-Fi is the upcoming and on growing technology acting as competent for various other developing and already invented technologies. Hence the future applications of the Li-Fi can be predicted and extended to different platforms and various walks of human life

References

[1] Aman Sodhi and Jeslin Johnson, "Light Fidelity (LI-FI) - The Future of Visible Light Communication" International Journal of Engineering Research and General Science Volume 3, Issue 2, March-April, 2015, ISSN 2091-2730

[2] Arya.V., Priya.P., Resma Omanakuttan and Shilby Baby, "Lifi: The Future Technology in Wireless Communication" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 4, Issue 4, April 2015, ISSN (Print) 2320-3765

[3] Sonali Waje and Sandip Rahane, "Information Transmission System Based On a Light Sensor" Int. Journal of Engineering Research and Applications, Vol. 4, Issue 6(Version 6), June 2014, pp.213-215, ISSN : 2248-9622

[4] Mr. Prakash Chandra Behera and Mr. Chinmaya Dash, "Light Fidelity: Substitution Technique to Overcome Challenges In Radio wave Data Transmission Process" International Journal of Innovations & Advancement in Computer Science,Volume 4, Special Issue March 2015, , ISSN 2347 – 8616

[5] Er. Amritpal Singh, "Li-Fi: Light Fidelity Technology-A Review" International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 12, December 2015ISSN (Print) 2319 5940

[6] Jagsir Singh and Inderdeep Kaur Aulakh "Light Fidelity: A New Emerging Wireless Technology that uses the Light for Data Transmission" SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE) – EFES April 2015

[7] Ekta and Ranjeet Kaur, "Light Fidelity (LI-FI)-A Comprehensive Study" International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 3, Issue. 4, April 2014, pg.475 – 481,ISSN 2320–088X

[8]http://www.academia.edu/6996573/CSE_Study_Paper_on_._Li_Fi_Technology_The_latest_technology_in_wireless

[9] Nitin Vijaykumar Swami, "Li-Fi (LIGHT FIDELITY) – THE CHANGING SCENARIO OF WIRELESS COMMUNICATION" IJRET: International Journal of Research in Engineering and Technology, eISSN: 2319-1163, pISSN: 2321-7308

Texture Features for Image Retrieval

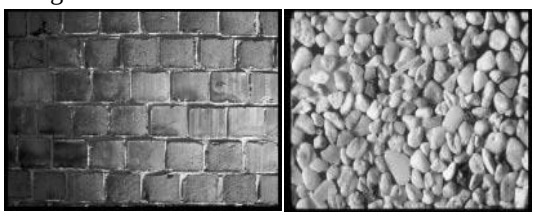
Komal Vijay[1], Pratap Singh Patwal[2]
[1]M.Tech Scholar, [2]Associate Professor, [3]Associate Professor
Department of Computer Science, Institute of Engineering & Technology, Alwar, Rajasthan

ABSTRACT
An ad hoc network is an aggregation of wireless nodes forming a provisional network without any established and central infrastructure. Mobile Ad-hoc Network (MANET) is an infrastructure less and decentralized network which need a robust dynamic routing protocol. Routing protocols helps node to send and receive packets. Routing is a challenging issue in MANET. A mobile system is characterized by the movement of its constituents. The mobility model is designed to describe the movement pattern of mobile users, and shows how their location, velocity and acceleration changes over time. Mobility patterns used to determine the protocol performance. The study of Mobility Models and their realistic vehicular model deployment is a challenging task. It tries to illustrate the behavior of a real world object.

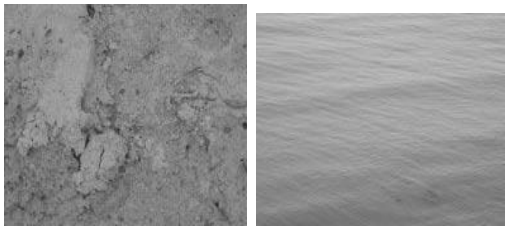
Keywords: AOD, DSR, RWP, RPGM

1. Introduction

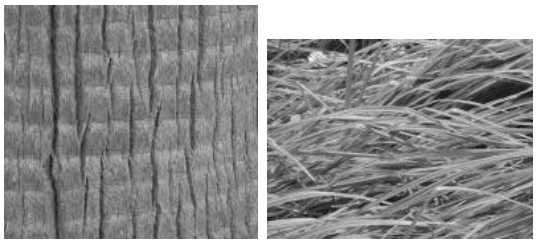
Texture is a property of image regions. It is easy to visualize. One can think of a texture as consisting of some basic Primitives whose spatial distribution in the image creates the appearance of a texture. Most Man-made objects have such easily identifiable texels. The spatial distribution of texels could be regular (or periodic) or random. In Figure 1.(a), "brick" is a micro pattern in which particular distribution in a "brick-wall" image constitutes a structured pattern. The individual primitives need not be of the same size and shape, as illustrated by the bricks and pebbles textures. Well-defined micro patterns may not exist in many cases, such as pictures of sand on the beach, water, and clouds. Some examples of textured images are shown in Figure1.



(a)Brick Wall (b)Stones and Pebbles



(c) Sand (d) Water



(e) Tree Bark (f) Grass

Figure1. Examples of some textured images.

During the past three decades, Image-texture analysis has primarily focused on texture classification, texture segmentation, and texture synthesis. The objective of texture classification is to assign a unique label to each homogeneous region. Texture segmentation refers to computing a partitioning of the image, each of the partitions being homogeneous in some sense. Segmentation and classification often go together—classifying the individual pixels in the image produces segmentation. To generate texture that is perceptually indistinguishable from that of a provided example. Such synthesized textures can then be used in applications such as texture mapping. Texture mapping is used to generate surface details of synthesized objects.
In the emerging application area of content-based access to multimedia data, texture is considered as an important visual cue.

2. TEXTURE FEATURES

A texture feature captures one specific attribute of an image, such as coarseness, and a coarseness descriptor is used to represent that feature. The terms feature and

descriptor (of a feature) are often used synonymously, in the image processing and computer-vision literature.

During the 1970s the research mostly focused on statistical texture features for discrimination, and in the 1980s, there was considerable excitement and interest in generative models of textures. These models were used for both texture synthesis and texture classification.

Human Texture Perception

Texture, is the basic visual feature, which helps in the studying and understanding of early visual mechanisms in human vision.

Julesz defines a "preattentive visual system" as one that "cannot process complex forms, yet can, almost instantaneously, without effort or scrutiny, detect differences in a few local conspicuous features, regardless of where they occur". Julesz coined the word *textons* to describe such features that include elongated blobs (together with their color, orientation, length, and width), line terminations, and crossings of line-segments. Differences in textons or in their density can only be pre-attentively discriminated.

Rao and Lohse identify three features as being important in human texture perception: repetition, orientation, and complexity. Repetition refers to periodic patterns and is often associated with regularity. A brick wall is a repetitive pattern, whereas a picture of ocean water is non-repetitive (and has no structure). Orientation refers to the presence or absence of directional textures. Complexity refers to the description complexity of the textures and, as the author state ". . . if one had to describe the texture symbolically, it (complexity) indicates how complex the resulting description would be." Complexity is related to Tamura's coarseness feature.

TEXTURE FEATURES BASED ON SPATIAL-DOMAIN ANALYSIS

Co-occurrence Matrices

Co occurrence matrices are based on second-order statistics of pairs of intensity values of pixels in an image. It counts how often pairs of grey levels of pixels, separated by a certain distance and lying along certain direction, occur in an image.

Let $(x, y) \in \{1,\ldots, N\}$ be the intensity value of an image pixel at (x, y).

Let $[(x1 - x2)2 + (y1 - y2)2]1/2 = d$, be the distance that separates two pixels at locations $(x1, y1)$ and $(x2, y2)$, respectively, and with intensities i and j, respectively. The co-occurrence matrices for a given d are defined as follows:

$$c(d) = [c(i, j)],\ i, j, \in \{1, \ldots, N\}$$

Where c (i, j) is the cardinality of the set of pixel pairs that satisfy **I** (x1, y1) =i and I (x2, y2) = j , and are separated by a distance d.

Tamura's Features

One of the influential works on texture features that correspond to human texture perception is the paper by Tamura, Mori, and Yamawaki. They characterized image texture along the dimensions of coarseness, contrast, directionality, line-likeness, regularity, and roughness.

Coarseness: It corresponds to the "scale" or image resolution. It also refers to the size of the underlying

Contrast: Contrast measures the amount of local intensity variation present in an image. It also refers to the overall picture quality—a high contrast picture is often considered to be of better quality than a low–contrast version.

Directionality: It is a global texture property. The degree of directionality, measured on a scale of 0 to 1, can be used as a descriptor.

AUTOREGRESSIVE AND RANDOM FIELD TEXTURE MODELS

Wold Model

For image retrieval application Liu and Picard propose the Wold model. It is based on Wold decomposition of stationary stochastic processes. In this model, a 2D homogeneous random field is decomposed into three mutually orthogonal components, which approximately correspond to the three dimensions (periodicity, directionality, and complexity or randomness). The construction of the Wold model proceeds as follows. First, the periodicity of the texture pattern is analyzed by considering the autocorrelation function of the image. The corresponding Wold feature set consists of the frequencies and the magnitudes of the harmonic spectral peaks. For similarity retrieval, two separate sets of ordered retrievals are computed, one using the harmonic-peak matching and the other using the distances between the MRSAR features. Then, a weighted ordering is computed using the confidence measure (the posterior probability) on the query pattern's regularity.

The experimental results in the Brodatz database, shows that the Wold model provides perceptually better quality results than the MRSAR model.

SPATIAL FREQUENCY AND TRANSFORM DOMAIN FEATURES

The last decade has seen significant progress in multi resolution analysis of images, and much work has been done on the use of multi resolution features to characterize image texture. Two of the more popular approaches have

been reviewed, one based on orthogonal wavelet transforms and the other based on Gabor filtering, which appear very promising in the context of image retrieval. Conceptually, these features characterize the distribution of oriented edges in the image at multiple scales.

Wavelet Features

Wavelet Transform is a multi resolution approach. Wavelet transforms refer to the decomposition of a signal with a family of basic functions obtained through translation and dilation of a special function called the mother wavelet. Two types of wavelet transforms have been used for texture analysis, the pyramid-structured wavelet transform (PWT) and the tree-structured wavelet transforms (TWT).

The computation of 2D wavelet transforms involves recursive filtering and sub sampling; and at each level, it decomposes a 2D signal into four sub bands, which are often referred to as LL, LH, HL, and HH, according to their frequency characteristics (L = Low, H = High).

Gabor Features

Gabor features have been used in several image-analysis applications, including texture classification and segmentation, image recognition, image registration, and motion tracking.

3. COMPARISON OF DIFFERENT TEXTURE FEATURES FOR IMAGE RETRIEVAL

Similarity Measures for Textures

For searching similar patterns in a large database systems texture descriptors are quite useful. In a typical "query-by-example" scenario, the user would be interested in retrieving several similar images and not just the best match. This requires comparing two descriptors to obtain a measure of similarity (or dissimilarity) between the two image patterns.

A Comparison of Texture Descriptors for Image Retrieval

The image database used consists of 19,800 *color natural images* from Corel photo galleries and 116 512 × 512 texture images from the Brodatz album and the USC texture database.

Corel photo database is used to evaluate the performance of texture features. The texture features with performance ordered from the best to the worst are: MRSAR (using image dependent covariance), Gabor, TWT, PWT, MRSAR (using global covariance), modified Tamura coarseness histogram and directionality, canny edge histogram, and traditional Tamura features.

In addition to the Corel photo database, the Brodatz texture album was also used to evaluate the performance of texture features. The features with performance ordered from the best to the worst are Gabor, MRSAR (using image-dependent covariance), TWT, PWT, modified Tamura, MRSAR (using global covariance), traditional Tamura, coarseness histogram, directionality, and canny edge histogram.

4. CONCLUSION

In applications such as segmentation and image retrieval, as low level descriptors of visual data, texture continues to play an important role. The numerous references provide pointers to the rich and diverse literature on image texture for further exploration of this very interesting and exciting topic.

References

[1] P. Brodatz, *Textures: A Photographic Album for Artists and Designers*, Dover Publications, New York, 1966.

[2] B. Julesz, Textons, the elements of texture perception, and their interactions, *Nature* 290(12), 91–97 (1981).

[3} B. Julesz and J.R. Bergen, Textons, the fundamental elements in preattentive vision and perception of textures, *Bell Syst. Tech. J.* **62**(6), 1619–1645 (1983).

[4] R.M. Haralick, Statistical and structural approaches to texture, *Proc. IEEE* **67**(5), 786–804 (1979).

[5] J.D. Foley et al., *Introduction to Computer Graphics*, Addison-Wesley, Reading, Boston, Mass., 1993.

[6] MPEG/ISO *Document N3349, MPEG-7 Overview*, Noordwijkerhout Netherlands, J. Martinez, ed., March 2000.

[7] R.M. Haralick and L.G. Shapiro, *Computer and Robot Vision (Vol. I)*, Addison- Wesley, Reading, Boston, Mass., 1992.

[8] B. Julesz, Visual pattern discrimination, *IRE Trans. Inf. Theory*, IT-8 84–92 (1961).

[9] S. Chatterjee and R. Chellappa, Maximum likelihood texture segmentation using Gaussian Markov random field models, *Proceedings of IEEE International Conference on Computer Vision and Pattern Recognition*, San Francisco, Calif., June 1985.

[10] F.S. Cohen and D.B. Cooper, Simple parallel hierarchical and relaxation algorithms for segmenting no causal Markovian fields, *IEEE Trans. Pattern Anal. Machine Intell.* **9**, 195–219 (1987).

DNA Technology: The Technology of Justice

Priyanka Vijay[1], Pratap Singh Patwal[2] Rohit Singhal[3]
[1]B.Tech Scholar, [2]Associate Professor, [3]Associate Professor
Department of Computer Science, Institute of Engineering & Technology, Alwar, Rajasthan

Abstract

From the beginning of this world the intelligence of human being, has resulted in the growth of science and technology. Science and technology are having tremendous impact on human lives. Advances in DNA technology are being seen as significant, reliable, efficient and accurate tools for law enforcement agencies to fight crimes. The DNA evidences have the ability of proving guilt of accused or innocence of accused persons who are wrongly convicted. Forensic DNA Technology has transformed investigative methods of serious crimes due to its remarkable capability to convict wrongdoers or exonerate accused or convicted offenders. Solving the cold cases is the most significant and great qualities of DNA evidence. More importantly, DNA technology can quickly lead suspicion away by allowing samples of past crimes that were never solved to be reassessed. This will result in the arrest of the suspect(s) years after the crime was committed. In essence, DNA evidence is rapidly becoming irrefutable proof of identification. The question whether DNA is advancing justice becomes relevant in cases where police, in their efforts, use DNA evidence to find suspects and solve crimes. Certainly, questions of justice weigh most heavily when the DNA samples of innocent person is taken, stored and analyzed and falls under the lens of suspicion. Therefore, this paper deals with the utility of DNA Technology in criminal investigation and advancement of DNA technology towards the vision of justice is the focal point of this research paper

Keywords

Forensic DNA technology, DNA evidence, technology of justice, cold case, criminal investigation.

1. Introduction

Now a day's perpetrators use science and technology as their advantage in committing crimes. Consequently, investigating officers are required to possess scientific tools to investigate these crimes.

Forensic science comes to their rescue by introducing DNA technology in the legal system. Forensic science is the application of principles of science and technology in investigation of crime(s) to enable the courts to determine the guilt of the accused. It is applied in both criminal as well as civil cases. The evolution of science and technology has enabled law enforcement agencies to solve many apparently 'unsolvable crimes', which have made people to associate forensic science with detection of crimes. Applications of DNA evidence assist the courts in determining, whether a crime in fact has been committed, and if it has been committed how and when. This article considers the likely impact of DNA technology on administration of criminal justice. It focuses on two major things of DNA technology: the utility of DNA test as powerful tool for identification purposes in criminal cases and admissibility of DNA samples recovered from the crime scenes in the courtroom.

DNA is generally used to solve crimes in one of two ways. In cases where a suspect is identified, a sample of that person's DNA can be compared to evidence from the crime scene. The results of this comparison may help establish whether the suspect committed the crime. In cases where a suspect has not yet been identified, biological evidence from the crime scene can be analyzed and compared to offender profiles in DNA databases to help identify the perpetrator. Crime scene evidence can also be linked to other crime scenes through the use of DNA databases.

In the Beginning: The forensic use of DNA started with the work of Alec Jeffreys, in 1984, Jeffreys invented the techniques which uses human biological sample in courtroom. He demonstrated that DNA samples, dried stains several years old, contained sufficient DNA to produce conclusive results. Jeffreys proved that even small fragments of DNA molecules were virtually unique to individuals

What is DNA: DNA is the abbreviation for deoxyribonucleic acid, which is the genetic material present in the cells of all living organisms. DNA is the fundamental building block for an individual's entire genetic makeup. DNA is found in almost every cells of human body such as blood, semen, urine, saliva, hair, etc. Every individual has unique DNA which does not match with others except monozygotic twins. Our body's cells each contain a complete sample of our DNA. The DNA in a person's saliva is the same in every skin cells, semen, etc.

2. Utility of DNA evidence as a powerful tool in criminal investigation: The uniqueness of DNA evidence makes it a powerful tool in criminal investigation, because, each person's DNA is unique except identical twins. Therefore, DNA evidence collected from a scene of crime can involve or exempt a suspect. Not only that, it can also examine unidentified remains of dead body with comparison of DNA from family members. Moreover, once DNA evidence from one scene of crime is compared with evidence from another using DNA database such as codis in us, those crime scenes can be connected to the same perpetrator locally, state wide and nationally. DNA test is also a powerful tool because when biological sample from scene of crime is collected and stored properly, forensically valuable DNA can be found on thing that may be decades old. Therefore, old cases that were previously thought unsolvable may be solved by DNA evidences because they are capable of identifying the perpetrator. The possible influence of DNA technology in investigation of crime is not seen in number of cases in court, because, a lot of its impact is behind the screens, such as exempting person from the gallows of suspects which lessens the court work-load when identity is found. The use of DNA evidence in crime cases is of paramount consideration, because it is a reliable investigative tool for exempting persons wrongly suspected of taking part in a crime. Not only that, DNA can also furnish convincing evidence of participation and the result of the analysis may induce the accused to plead guilty. In criminal investigation, the presence of DNA evidence is deemed to have an effect on the confession made by suspects.

Admissibility of DNA evidence in litigation: The service of criminal justice system often uses scientific expert and forensic DNA evidence in investigation. DNA testing is used to find out the connection between biological sample found at crime scene and suspect. It can also be used to establish whether the fingerprints found on a gun is for the accused party. The qualification of DNA evidence to be reliable for use must be proper preservation of sample by competent forensic expert(s) or trained police in that area. A DNA sample that is badly smudged when found cannot be usefully saved or analyzed it may even mislead investigation in case of contamination.

The issue of admissibility of DNA evidence is crucial. While presenting the DNA evidence there should be balance between legal rights of the suspect as against the interest of the state. This is the main reason to support the conformity required by law leading to accurate collection of DNA samples. The power is in the hands of judiciary to consider or not to consider DNA evidence after weighing the prejudices against probative values.

Every court of law has discretionary power to refute DNA evidence obtained in situations which may cause to be used against the accused in unjustly manner8. The exercises of the discretionary power of the court for the sake of justice, the courts balance public interest in prosecution of wrongdoers or perpetrators, as against the public interest in the protection of the individual from illegal and unjust treatment. While DNA evidence is acquired in breach of stipulated scientific process, the court can admit the questionable evidence simply when the necessity of admitting the evidence prevails over the undesirability of admitting it. The problem of admissibility of DNA evidence is nevertheless, an issue which has to be regulated under domestic law.

During the period of 20th century, as science developed, the legal system was not developing keeping pace with evolution of science to admit scientific evidence in the system of justice9. The first remarkable case in United States was *frye v. United States10*. In this murder case, the suspect wanted to prove his innocence through lie detection test, unfortunately court rejected his wish on ground that, the evidence must be well recognized by scientific principle or discovery and the thing from which the deduction is made must be sufficiently ascertained and secure the general acceptance in particular field in which it belong11.

However, the first daring case that had an impact on DNA evidence was *people v. Castro12*, wherein admission of DNA evidence was examined vigorously in this case. A blood stain was found on Jose Castro's watch accused of murdering his neighbour and her daughter. After analyzing the blood stain found on Castro's watch, the court concluded that the theory underlying DNA test is generally accepted by scientists in genetics and the techniques applied in the particular case were so faulty, hence, evidence of a match is inadmissible13. After establishing that forensic DNA evidence met the principles led down under *frye*, the court set up a new standard for the admissibility of DNA evidence, not only that DNA test is generally accepted in scientific community but, also to establish that the technique and procedure were properly followed by laboratories in specific case before the court.

In India, quite a few convictions have occurred wherein DNA evidence has been indirectly acknowledged under

section 45 of the Indian evidence act, 187215. Section 45 of the said act deals directly with the opinion of the expert stating that "when the court has to form an opinion upon a point of foreign law, or science or art, or as to identity of handwriting (or finger impressions), the opinions upon that point of persons specially skilled in such foreign law, science or art, (or in questions as to the identity of handwriting or finger impressions) are relevant facts."

The courts held that medical evidence is only an evidence of opinion and is hardly decisive. It is not substantive evidence. But, the opinion of the doctor who has held the postmortem examination and of the forensic science laboratory is reliable. The supreme court of India has further stated that unless there is something inherently defective in the medical report, the court cannot substitute its own opinion for that of the doctor16.

The reports of certain government scientific experts are dealt under section 293 of the code of criminal procedure. Section 293(2) stipules that when the court thinks necessary can scrutinize the report given by the expert. The court should not take that report as it is without making an analysis17. People have different views regarding fundamental principle of scientific evidence like DNA evidence for instance; it cannot be subjected or questioned, only legal analysis should be done on collection and authentication of scientific samples18.

Nevertheless, a number of writers believe that, there are no national or international standards; each laboratory has its own guiding principles. However, the court is not likely to comprehend in minute details the standards of the process; the court considers the opinion of the expert based on trust19. In addition, various courts are still hesitating to admit DNA evidence as they are of opinion that laboratories are not following the general scientific principles or this violates fundamental principles and public policy.

Therefore, in India, there is still uncertainty on what criteria and laws the courts should be based on for the admission of DNA evidence. The capability of DNA evidence to establish innocence or guilt of crime beyond reasonable doubt is being acknowledged by judiciary in various countries. India is not lugging behind, although DNA technology has not yet being fully welcomed in investigation process and justice delivery system. Gradually, India is acknowledging the outcome of DNA testing, it is moving toward passing of legislation which will deal with DNA technology and set up of DNA database. Additionally, Indian judiciary has passed various decisions based on DNA evidences.

Toward a vision of technology of justice: The vision of justice to which the criminal justice system is based on; should be a proper balance between the protection of civil liberties, presumed innocence, and procedural rights of persons and the needs of the state to apprehend, punish and rehabilitate perpetrators of crime. People have an expectation of privacy in respect to the content of their DNA sample, regardless of where it has been obtained or acquired. The issue arises when DNA of an individual is analyzed beyond the identification purpose.

In hiibel v. Nevada, us supreme court held that, a person does not have a constitutional right to withhold his or her identity. But the police cannot stop a person without reasonable suspicion simply to acquire the individual's identity. Hence, to reiterate from the said case, even if DNA evidences were used exclusively for identification purpose, there are still limits on what police can do to obtain DNA identity. Law enforcement agencies have to meet legally justified cause or reasonable suspicion requirement to acquire DNA evidence. It is very significant to note that DNA is not simply being collected for identification purpose only but also for investigation, inculpatory and exculpatory purposes.

3. Evolving impact of DNA technology on the criminal justice system: Evolution of DNA technology is having a major impact on laws as they have or are being amended in much legislation worldwide. This affects the way investigations are done and how to handle unsolved cases. Its innovation is of supreme consideration because laws are being enacted, amended, and repelled even altered to maximize the benefits of the ability of DNA technology to identify, convict and exempt innocent falsely convicted24. Enactment of law regarding the collection, use, storage, admissibility and creation of DNA database for DNA evidence reflects the impact of DNA technology on criminal justice system. The legal provisions of limitation limit the time within which criminal charges can be filed for a particular offence.

Those provisions are deep-rooted in laws prohibiting the person from utilizing the evidence that has turned out to be outdated over a period of time. For instance, an eye-witness may forget the detail(s) of what he has seen due the laps of long time; his memories vanish as time passes. However, DNA evidence is a powerful and reliable tool which can

establish the truth with accuracy regardless decades after the crime was committed.

The irrefutable achievement of DNA technology is that it has resulted in general tendency towards the creation of DNA database in other countries which have established national DNA database system. Even though DNA evidence is not the only tool that helps to solve unsolved cases, evolution of DNA technology and the achievement of DNA database have instigated the law enforcement agencies to reassess the so called "cold cases". Nowadays, investigating officers have realized the ability of DNA evidence to easily identify a suspect in ways previously seen as impracticable or unrealistic. The visible evidence to the naked eye can be used in settlement of some crimes, but because the perpetrators are using the umbrella of technology to commit crime, DNA technology is playing remarkable role to solve that crime25.
Laws are being enacted in various countries to call for all convicted felons to surrender their DNA sample for the creation of DNA profile to be stored into state DNA database. The more DNA samples are submitted the larger the DNA database, rendering database system a more powerful tool for law enforcement.

Stimulating Research and Development: In order to improve the use of DNA technology to advance the cause of justice, the Attorney General will stimulate research and development of new methods of analysing DNA samples under the President's initiative. Also, the president has asked the Attorney General to establish demonstration projects under the initiative to further study the public safety and law enforcement benefits of fully integrating the use of DNA technology to solve crimes. Finally, the president has directed the Attorney General to create a National Forensic Science Commission to study rapidly evolving advances in all areas of the forensic sciences Commission to study rapidly evolving advances in all areas of the forensic sciences and to make recommendations to maximize the use of the forensic sciences in the criminal justice system. In all, the president's initiative will devote $24.8 million in FY 2004 to fund advances in the use of DNA technology.

Improving DNA Technology: Forensic DNA analysis is rapidly evolving. Research and development of tools that will permit crime laboratories to conduct DNA analysis quickly is vital to the goal of improving the timely analysis of DNA samples. Smaller, faster, and less costly analysis tools will reduce capital investments for crime laboratories while increasing their capacity to process more cases. Over the course of the next several years, DNA research efforts will focus on the following areas:

- The development of "DNA chip technology" that uses nanotechnology to improve both speed and resolution of DNA evidence analysis. This technology will reduce analysis time from several hours to several minutes and provide cost-effective miniaturized components.
- The development of more robust methods to enable more crime labs to have greater success in the analysis of degraded, old, or compromised items of biological evidence.
- Advanced applications of various DNA analysis methods, such as automated Short Tandem Repeats (STRs), Single Nucleotide Polymorphisms (SNPs), mitochondrial DNA analysis (mtDNA), and Y-chromosome DNA analysis.
- The use of animal, plant, and microbial DNA to provide leads that may link DNA found on or near human perpetrators or victims to the actual perpetrator of the crime.
- Technologies that will enable DNA identification of vast numbers of samples occasioned by a mass disaster or mass fatality incident.
- Technologies that permit better separation of minute traces of male sexual assailant DNA from female victims.

The initiative devotes $10 million in FY 2004 funding to benefit the state and local criminal justice community through DNA research and development. It also requests $9.8 million in FY 2004 funding to further expand the FBI's DNA research and development program.

4. Conclusion

DNA evolution has drawn attention of judiciary, to focus on evaluation and admission of DNA technology into legal systems. Various decisions such as *daubert* in usa, gave confidence to the judges to exercise greater freedom to appraise scientific evidence which would help to resolve remaining issues of admissibility. In due course, absolute acceptance of existing and praiseworthy of new DNA principles is certain. For that reason these investigative tools will merely turn out to be greater than they are nowadays. Meanwhile, judges should not be reluctant to accept DNA technology to be incorporated in justice

system while waiting for suitable answers to the issues raised by it. Judges should not miss out the best way of interpreting the results of DNA testing because there will be most likely discussion over the perfect way of interpretation and analysis of DNA results among judges and scientists. Justice delayed is justice denied, and DNA technology has proved to be constructing and helpful in justice delivery system. The investigation process needs to be hastened by acknowledging DNA evidence as powerful tool of current and future need; otherwise the criminal justice system will suffer.

When used to its full potential, DNA evidence will help solve and may even prevent some of the Nation's most serious violent crimes. However, the current federal and state DNA collection and analysis system needs improvement:

1. In many instances, public crime labs are overwhelmed by backlogs of unanalyzed DNA samples.
2. In addition, these labs may be ill-equipped to handle the increasing influx of DNA samples and evidence. The problems of backlogs and lack of up-to-date technology result in significant delays in the administration of justice.
3. More research is needed to develop faster methods for analyzing DNA evidence.
4. Professionals working in the criminal justice system need additional training and assistance in order to ensure the optimal use of DNA evidence to solve crimes and assist victims.

The current federal and state DNA collection and analysis system needs improvement. In many instances, public crime labs are overwhelmed by backlogs of unanalyzed DNA samples. In addition, these labs may be ill-equipped to handle the increasing influx of DNA samples and evidence. The problems of backlogs and the lack of up-to-date technology result in significant delays in the administration of justice. More research is needed to develop faster methods for analyzing DNA evidence. Professionals involved in the criminal justice system need additional training and assistance in order to ensure the optimal use of DNA evidence to solve crimes and assist victims. And the criminal justice system needs the means to provide DNA testing in appropriate circumstances for individuals who assert that they have been wrongly convicted

References

[1] Yawer Qazalbash, DNA Evidence and Its Admissibility, 24 (**2006)**

[2] Parikh and Mishra, The principles of Medical Jurisprudence, Medical and Forensic Science, DNA test and Toxicology,11**(2007)**

[3] The CODIS Unit manages the Combined DNA Index System (CODIS) and the National DNA Index System (NDIS) and is responsible for developing, providing, and supporting the CODIS Program to federal, state, and local crime laboratories in the United States and selected international law enforcement crime laboratories to foster the exchange and comparison of forensic DNA evidence from violent crime investigations, **(2010)**

[4] Sheldon Krimsky and Tania Simoncelli, Genetic Justice: DNA data banks, Criminal Investigations, and civil liberties, 306-307 **(2011)**

[5] Edward Connors, Convicted by jury exonerated by Science, *IPT Journal*, **(10) (1998)**

[6] Abichandani R.K., New Biology and Criminal Investigation, **(2010)**

[7] Sharma Abhijeet, Guide to DNA Test in Paternity Determination and Criminal Investigation, 260 **(2007)**

[8] Heydon J.D., Cross on Evidence, 795, **(2000)**

[9] http://www.nap.edu/openbook.php?record_id. visited on 11th Sept, **(2010)**

[10] 293 F. 1013, 1014, D.C. Cir, **(1923)**

[11] The *Frye* decision was that the lie detector test was not trustworthy for the reason that it had not obtained "general acceptance" in the relevant scientific community. Its meaning test is indefinable. In fact, the *Frye* test brought a lot of debate in by Judges, whether the scientific evidence should be admitted in legal system or not. For many years, the *Frye* test was cited in both civil and criminal cases, but it was applied most frequently in criminal cases, **(1923)**

[12] 447NW422, Minn **(1989)**

[13] The Castro judgment provides the intention that DNA identification evidence of exclusion is more providing reasonable basis of admissibility than DNA identification evidence of *inclusion*. In Castro, the court ruled that DNA tests could be used to show that blood on Castro's watch was not his, but tests could not be used to show that the blood was that of his victim, Accessed on 14th June, 2010, *See also,* DNA Technology in Forensic Science, Committee on DNA Technology in Forensic Science, USA Board of Biology, Commission on Life Science, National Research Council of USA **(1992)**

[14] Adhikary Jyotimor, DNA Technology in Administration of Justice,56-57 **(2007)**

[15] KSN Reddy, The Essentials of Forensic Medicine and Toxicology, 387 **(2004)**

[16] Kantak M.P., Ghodkirekar M.S. and Perni S.G., Utility of Daubert guidelines in India, Journal of the Indian Academy of Forensic Medicine, **26 (2004)**

[17] Madan Gopal Kakkad vs. Naval Dubey and another 3 SSC 204 **(1992)**

[18] Pillay V.V., Textbook of Forensic Medicine and Toxicology, 14th ed., **89** (**2004)**

[19] Vij K., Textbook of Forensic Medicine (Principles and Practice). 1st ed., **134 (2001)**

[20] State of Gujarat v. Kishnbhai, MANU/GJ/0506 /2005 (In this case the police was criticized for not having employed DNA test during investigation. It was observed, in case of rape, where injuries on the vagina of the victim are so grave and serious, in our opinion, either pubic hair or semen of the accused ought to have been found from the body of the victim.

[21] R.R. Gopal v. State of Tamil Nadu,AIR1997 SC 264,

[22] 542 U.S. 177, **(2004)**

[23] Hiibel v. Sixth Judicial District Court of Nevada, Humboldt Country et al., U.S. Supreme Court, NO03-5554, decided June, 2 **(2004)**

[24] National Institute of Justice (NIJ), Convicted by Juries Exonerated by Science, Case study in using DNA evidence to establish innocence after trial. Report released, (**2009)**

[25] Susan Price Livingston, D*NA Database of Convicted Felons*, OLR Research Report, **(2002)**

[26] Special Report on, Using DNA to Solved Cold Cases, published by the National Institute of Justice (U.S. Department of Justice), **(2002)**

[27] http://www.justice.gov/ag/advancing-justice-through-dna-technology-executive-summary.

[28] http://www.justice.gov/ag/advancing-justice-through-dna-technology-using-dna-solve-crimes

[29] http://nij.gov/topics/forensics/evidence/dna/dna-initiative/Pages/welcome.aspx

[30] http://www.justice.gov/ag/advancing-justice-through-dna-technology.

Review Paper on Image Encryption with Pipelining Pixel Scrambling and Fractional Fourier Transform

Sunita Kumari[1],Pratap Singh Patwal[2],Dr.A.K. Srivastava[3]

[1]M.Tech Scholar, [2]Associate Professor,[3]Director(Prof)

Department of Computer Science, Institute of Engineering & Technology, Alwar[1]

SGV University, Jaipur[2], Director RGGI, Meerut[3]

ABSTRACT-

In recent years the use of networks has grown tremendously. Digital information is transmitted through internet. In recent years security of information is of prime importance and encryption is the best method to provide security.A review paper on image encryption based on fractional Fourier transforms (FRFT) is described and demonstrated in this paper. Numerical simulation results are given to verify the algorithm. Here in this paper we will show the use of fractional Fourier transform for encrypting images.

Keywords: FT, FRFT, Encryption.

1. Introduction

According to the cryptography, encryption is a way of transforming any sensitive information using an algorithm (called a cipher) to make it unreadable to anyone except those possessing extraordinary information, more often than not referred as key. The reverse process, i.e., to make the encrypted information readable again, is referred to as decryption (i.e., to make it unencrypted). The use of encryption in military applications to facilitate secret communication is known fact. But now it is commonly used in securing data within various kinds of national system. With the evolution of internet and the increase in the necessity for image transmission, information security and data encryption are becoming more and more important. Encryption systems using Fourier transform have recently caught eyes for the multiple advantages of processing complex two-dimensional data in parallel and transmitting at great speed [1]. Fourier transform is widely used in signal processing system. The fractional Fourier transform (FRFT) is new generation of the conventional Fourier transform with a transform order parameter α, which may be integer or fraction. In every field where Fourier transform is used, the processing effect can be greatly improved by using FRFT. Many researches on data encryption with FRFT have been reported [5,14]. Unni krishnan et al. [5,6] encoded a primary image to stationary white noise by using two statistically independent random phase masks in fractional Fourier domains. Nishchal et al. [7] proposed a full phase encryption system, where the encrypted image was holo graphically recorded in a barium titanate crystal and then was decrypted by generating through phase conjugation. Nishchal et al. [10] used FRT in digital holography, that is, the encrypted data and the decryption key were recorded as digital holograms. Full digital technique used in this method enabled digital storage, transmission, and decryption of encrypted data. N.K.Nischal, J.Joseph and K.Singh [2] advised that full phase encryption can be done by using Fractional Fourier Transform. A new type of algorithm is suggested. This algorithm applies random phase encoding to encrypt images. The images are encrypted by applying correct keys. The keys are of fractional orders. The decryption is vice versa of encryption. The phase-based image by means of a muscular key space is additional sensitive to keys and turbulence than the amplitude-based image. The pixel scrambling process enhances the quality of the decrypted image. This technique is verified by simulations. C.C.Shih [3] He investigated FRFT, that is fractionalization of Fourier for encryption of two descriptions into inactive white noise. The mixture of the mixture complex signal from the twice primary real valued images involve the fully phase encoding and pixel scrambling techniques. G, Unnikrishnan, J.Joseph K.Singh [9] Random fractional Fourier transforms is being used. The same rules can be practical to create a novel type of fractional order Fourier transform which results in a smooth conversion of a function when transformed connecting the real and Fourier spaces, while this fresh approach does not mainly depend on the property of Fourier transform, it can be with no trouble generalized for any previous discrete periodic mathematical operation.Hennelly and Sheridan [11] demonstrated a new method based on random shifting of different sections of the original image in fractional Fourier domains, which shows superior, compared with available methods, at least comparable robustness to blind decryption. Nishchal et al. [14] performed a jigsaw

transform with diffractive optical element and a localized fractional Fourier transform on the original image, in which two random phase masks are used to encrypt the image to a stationary white noise. The jigsaw transform index and the number of image segments should be equal. Otherwise, the jigsaw has to be done digitally on the original image[14]. The size of different segments is limited by the diffractive elements manufacture processing and could not be small enough

2. DEFINITION OF FRFT

FRFT is a generalization of FT [1, 15]. It is not only richer in theory and more flexible in application, but is also not expensive in implementation. It is a powerful tool for the analysis of time-varying signals. With the advent of FRFT and related concepts, it is seen that the properties and applications of the conventional FT are special cases of those of the FRFT. However, in every area where FT and frequency domain concepts are used, there exists the potential for generalization and implementation by using FRFT. Mathematically, α th order FRFT is the α th power of FT operator. Hence α th order FRFT of any signal $s(t) \in L(R^2)$ is given by.

$$F^{\alpha}[s(t)] = \int_{-\infty}^{+\infty} s(t)K(\alpha;\omega,t)dt \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

Where

$$K(\alpha;\omega,t) = K(\alpha)\exp[(B(\alpha)\omega^2 - C(\alpha)\omega t + B(\alpha)t^2)] \quad \ldots\ldots (2)$$

Is the kernel of F^{α}, α is the fraction, and

$$K(\alpha) = \sqrt{\frac{[1 - j\cot(\alpha)]}{2\pi}} \quad \ldots\ldots\ldots\ldots\ldots\ldots (3)$$

$$B(\alpha) = \cot(\alpha) \quad \ldots\ldots\ldots\ldots\ldots\ldots (4)$$

$$C(\alpha) = \frac{1}{\sin(\alpha)} \quad \ldots\ldots\ldots\ldots\ldots\ldots (5)$$

$$\alpha = \frac{\pi a}{2} \quad \ldots\ldots\ldots\ldots\ldots\ldots (6)$$

For integer values of α it can be deduced that my fractional Fourier transform repeat itself at an interval of 4 that can be shown as

$$F^{4m+l}[s(t)] = F^{l}[s(t)] \quad \ldots\ldots\ldots\ldots\ldots\ldots (7)$$

Where *m* is any integer and *l* can be any real number.

3. .IMAGE ENCRYPTION USING FRFT

The use of fractional Fourier transform in the image encryption is been implemented in various paper. It is simple process of encryption which will take an image and take the two dimensional fractional Fourier transform it. So the image will get converted in to unreadable form. To get back the image just take the inverse fractional Fourier transform of the encrypted image.

Let $R_{n-1}(x,y)$ represent the primary normalized amplitude image to be encrypted. For encryption, the image will pass through the FRFT block as can be seen in Fig 1 and result in $R_n(x,y)$.

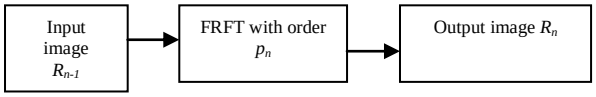


Fig. 1 Schematic of Image Encryption

So the final image equation will be.

$$R_n(x,y) = F^{\beta} \cdot [F^{\alpha}.\{R_{n-1}(x,y)\}] \quad \ldots\ldots\ldots\ldots (8)$$

Now from the Fig 3 as it can be seen that the input image $R_n(x,y)$ which is encrypted image will pass through the FRFT block and result in the original image $R_{n-1}(x,y)$.

So the final image equation at the receiver side will be

$$R_{n-1}(x,y) = [F^{-\beta} \cdot \{F^{-\alpha}.R_n(x,y)\}] \quad \ldots\ldots\ldots\ldots (9)$$

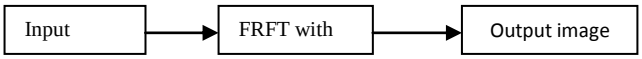


Fig. 2 Schematic of Image Decryption

4. Simulation Results

Computer simulations are performed to verify the proposed encryption technique for image encryption and decryption using MATLAB. Image of college gate can be seen in Fig.3, which serves as a primary image to be encrypted with the size of 308x308 pixels.

Fig. 3 Original Image

Now the order (α, β) which is used in FRFT for the image encryption is as follow *(4.9, 2.4)*. So the image after encryption can be seen in Fig 4.

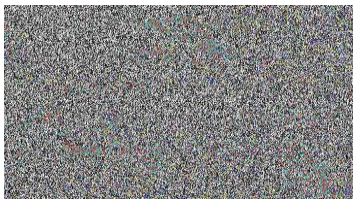


Fig. 4 Encrypted image after applying FRFT

To recover back image order $(-\alpha, -\beta)$ of FRFT is (-4.9,-2.4). And hence the image which is decrypted image or the original image can be seen in Fig 5.

Fig. 5 Decrypted Images after applying the reverse process

5. Conclusion

In the proposed encryption method order of the fractional Fourier transform served as the key and makes the encryption very efficient. The proposed encryption and decryption is implemented on one image to check the algorithm. We will devise a new method for image encryption with pipelining pixel scrambling and fractional fourier transform which will enhance the security system by 1000 times.

REFERENCES

[1] V. Namias, *"The fractional order Fourier transform and its application to quantum mechanics,"* J. Inst. Math. Appl., vol. 25, 1980, pp. 241–265.

[2] N. K. Nishchal, J. Joseph, and K. Singh, *"Fully phase encryption using fractional Fourier transform,"* Opt. Eng. 42, 1583–1588 (2003).

[3] C. C. Shih, *"Fractionalization of Fourier transform,"* Opt. Commun., no. 118, Aug. 1, 1995, pp. 495–498.

[4] G. Unnikrishnan and K. Singh, *" Random fractional Fourier domain encoding for optical security,"* Opt. Eng., vol. 39, 2000, pp. 2853–2859.

[5] Jun LANG , Ran TAO and Yue WANG, *"The Generalized Weighted Fractional Fourier Transform and Its Application to Image Encryption ,"* Image and Signal Processing, 2009. CISP '09. 2nd International Congress, IEEE, 978-1-4244-4131-0

[6] Ran Tao, Yi Xin, and YueWang,*"Image encryption based on random phase encoding in the fractional Fourier domain ,"*Optical Express-2007,Vol. 15, No. 24.[7] R. Tao, J. Lang, Y. Wang. *"Image encryption based on the multiple-parameter fractional Fourier transform,"* Opt. Lett. vol. 33, 2008, pp. 581-583.

[8] A. Sinha, K. Singh, "*Image encryption by using fractional Fourier transform and jigsaw transform in image bit planes,"* Opt. Eng. 44, 057001 (2005).

[9] G. Unnikrishnan, J. Joseph, and K. Singh, *"Optical encryption by random phase encoding in the fractional Fourier domain,"* Opt. Lett. 25, 887-889 (2000).

[10] N. K. Nishchal, G. Unnikrishnan, J. Joseph, and K. Singh, *"Optical encryption using a localized fractional Fourier transform,"* Opt. Eng. 42, 3566-3571, (2003).

[11] Z. Liu and S. Liu, *"Double image encryption based on iterative fractional Fourier transform,"* Opt. Commun. 275, 324–329 (2007).

[12] P. Refregier and B. Javidi, *"Optical image encryption based on input plane and Fourier plane random encoding,"* Opt. Lett., vol. 20, 1995, pp. 767–769.

[13] G. Situ and J. Zhang, *"Multiple-image encryption by wavelength multiplexing,"* Opt. Lett. 30, 1306-1308 (2005).

[14] G. Situ and J. Zhang, *"Position multiplexing for multiple-image encryption,"* J. Opt. A: Pure Appl. Opt. 8, 391 (2006).

[15] H. M. Ozaktas, Z. Zalevsky, and M. A. Kutay *"The Fractional Fourier Transform with Applications in Optics and Signal Processing"* New York: Wiley, 2000.

[16] N. K. Nishchal, J. Joseph, and K. Singh, *"Fully phase-based encryption using fractional order Fourier domain random phase encoding: Error analysis,"* Opt. Eng. 43, 2266-2273 (2004).

[17] N. Towghi, B. Javidi, and Z. Luo, *"Fully phase encrypted image processor,"* J. Opt. Soc. Am. A 16, 1915 (1999).

18] J. Zhao, H. Lu, X.S. Song, J.F. Li, and Y.H. Ma, *" Image encryption based on multistage fractional Fourier transforms and pixel scrambling technique,"* Opt. Commun. 249, 493-499, (2005).

[19] B. Javidi, N. Towghi, N. Maghzi, and S. C. Verrall, *"Error-reduction techniques and error analysis for fully phase- and amplitude-based encryption,"* Appl. Opt. 39, 4117–4130 (2000).

[20] J. Hua, L. Liu, and G. Li, *"Extended fractional Fourier transforms,"* J. Opt. Soc. Am. A 14, 3316-3322 (1997).

[21] A. W. Lohmann, *"Image rotation, Wigner rotation, and the fractional Fourier transform,"* J. Opt. Soc. Am. A 10, 2181- (1993

A Review of Face Recognition

Charu Aroro[1],Vinit Bhargava[2],Sourabh Banga[3]
[1]M.Tech Scholar, [2]Associate Professor, [3]Assistant Professor
Department of Computer Science, Institute of Engineering & Technology, Alwar, Rajasthan

ABSTRACT

Facial recognition can be known as a form of biometric detection done by scanning the face of a person and then comparing it against the database of known faces. For the past years, researchers and scholars of this field have evolved new methods. The rapid developments of face recognition are being fueled by numerous advances in computer vision. An ongoing challenge in this field is to design an effective human-computer interaction (HCI). Human beings can distinguish a particular face from many depending on a number of factors. One of the main objectives of computer vision is to create such a face recognition system that can emulate and eventually surpass this capability of humans. A robust face recognition system is a system based on good feature extractor method and good classifier.

Keywords: Face detection, Feature extraction, face recognition, Eigen faces, Face recognition, HCI.

1. INTRODUCTION

A facial recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a facial database. The human face plays a major role in conveying identity and emotion. It is typically used in

Security systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems. A notable advantage of facial recognition over other biometric recognition methods is that it is less cumbersome for end users. We do face recognition almost on a daily basis. Most of the time we look at a face and are able to recognize it instantaneously, if we are already familiar with the face. Presently available face detection methods mainly rely on two approaches. The first one is local face recognition system which uses facial features of a face e.g. nose, mouth, eyes etc. to associate the face with a person. The second approach or global face recognition system use the whole face to identify a person.

Face recognition has received significant attention in the last 15 years [3], due to the increasing number of commercial and law enforcement applications requiring reliable personal authentication (e.g. access control, surveillance of people in public places, security of transactions, mugs hot matching, and human-computer interaction) and the availability of low-cost recording devices. Face recognition, as one of the primary biometric technologies which became more important owing to rapid advances in technologies such as digital cameras, the internet and mobile devices, and increased demands on security [3].

Further the paper is organized as follows: section two describes a generic face recognition system, section three focuses on different face recognition algorithms and techniques, section recognition technology, finally the conclusion in the section five four discuss about the applications of face.

2. A GENERIC FACE RECOGNITION SYSTEM

Face recognition is one of the most relevant applications of image analysis. It's a true challenge to build an automated system which equals human ability to recognize faces. Although humans are quite good identifying known faces, we are not very skilled when we must deal with a large amount of unknown faces. The computers, with an almost limitless memory and computational speed, should overcome human's limitations. The face recognition techniques mainly work in three steps:

1. Face Detection
2. Feature Extraction
3. Face Recognition

- **Face Detection**

Face detection can be regarded as a specific case of object-class detection. In object-class detection, the task is to find the locations and sizes of all objects in an image that belong to a given class. Face detection can be regarded as a more general case of face localization. In face localization, the task is to find the locations and sizes of a known number of faces (usually one). In face detection, one does not have this additional information.

- **Feature Extraction**

The In pattern recognition and in image processing, feature extraction is a special form of dimensionality reduction. When the input data to an algorithm is too large to be processed and it is suspected to be notoriously redundant

then the input data will be transformed into a reduced representation set of features. After the FD step, human-face patches are extracted from images. Directly using these patches for FR have some disadvantages, first, each patch usually contains over 1000 pixels [3], which are too large to build a robust recognition system. Second, face patches may be taken from different camera alignments, with different face expressions, illuminations, and may suffer from occlusion and clutter. To overcome these drawbacks, feature extractions are performed to do information packing, dimension reduction, salience extraction, and noise cleaning. After this step, a face patch is usually transformed into a vector with fixed dimension or a set of fiducially points and their corresponding locations. Transforming the input data into the set of features is called feature extraction.

- **Face Recognition**

A facial recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a facial database. It is typically used in security systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems. Among the different biometric techniques, facial recognition may not be the most reliable and efficient. However, one key advantage is that it does not require aid (or consent) from the test subject [3][6]. Properly designed systems installed in airports, multiplexes, and other public places can identify individuals among the crowd.

3. ALGORITHMS & FOR FACE RECOGNITION

- **Principal Component Analysis (PCA) using Eigen faces.**

PCA is the simplest of the true eigenvector based multivariate analysis. Mathematically, it is an orthogonal linear transformation that transforms the data to a new coordinate system [14]. The use of Eigen faces is commonly called as Principal Component Analysis. With PCA, the image must be used of same size and they are normalized to line-up the eyes and mouth of the subjects within the image. Using PCA, dimension of

Data using data compression basics is reduced and precisely decompose the face structure into orthogonal and uncorrelated components known as Eigen faces. The face image can be represented as a weighted sum or feature vector of the Eigen faces which can be stored in a 1-D array.

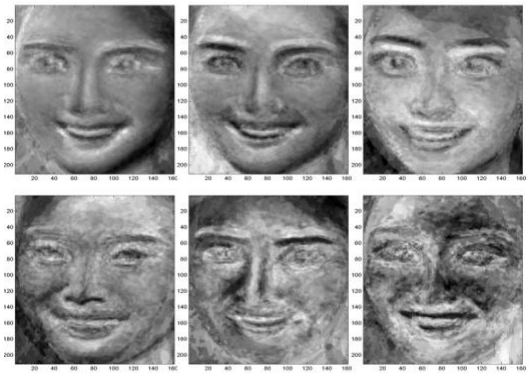


Fig 1: Standard Eigen Faces

- **Linear Discriminant Analysis (LDA)**

LDA is a statistical approach based on the same statistical principles as PCA. LDA classifies faces of unknown individuals based on a set of training images of known individuals. The technique finds the underlying vectors in the facial feature space (vectors) that would maximize the variance between individuals (or classes) and minimize the variance within a number of samples of the same person (i.e., within a class) [8]. If this can be achieved, then the algorithm would be able to discriminate between individuals and yet still recognize individuals in some varying conditions (minor variations in expression, rotation, illumination, etc.). If we look at Figure 2 we can see that there is a relatively large amount of variation between the individuals and small variations between the varieties of poses of the same individual.

Fig 2: Example of Variations between and within Classes

- **Elastic Bunch Graph Matching (EBGM)**

EBGM relies on the concept that real face images have many nonlinear characteristics that are not addressed by the linear analysis methods discussed earlier, such as variations in illumination (outdoor lighting vs. indoor fluorescent), pose (standing straight vs. leaning over) and expression(smile vs. frown). A Gabor wavelet transform creates a dynamic link architecture that projects the face

onto an elastic grid. The Gabor jet is a node on the elastic grid, notated by circles on the image below, which describes the image behavior around a given pixel. It is the result of a convolution of the image with a Gabor filter, which is used to detect shapes and to extract features using image processing. The success of Gabor filters is in the fact that they remove most of the variability in images due to variation in lighting and contrast. At the same time they are robust against small shifts and deformations. The Gabor filter representation increases the dimensions of the feature space (especially in places around key landmarks on the face such as the eyes, nose, and mouth) such that salient features can effectively be discriminated [12].

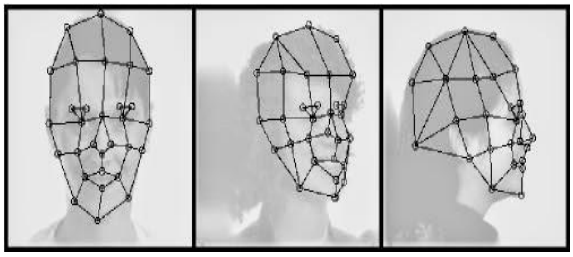


Fig 3: Elastic Bunch Graph Matching

4. FACE DETECTION TECHNIQUES

A huge number of representation techniques are available for face detection, including Knowledge-based, Feature invariant based, Template matching method, Appearance-based methods, Part-based methods, etc.

- **Knowledge-based methods**

These rule-based methods encode human knowledge [6] of what constitutes a typical face. Usually, the rules capture the relationships between facial features. These methods are designed mainly for face localization, which aims to determine the image position of a single face.

- **Feature invariant approaches**

These algorithms aim to find structural features that exist even when the pose, viewpoint, or lighting conditions vary, and then use these to locate faces. To distinguish from the knowledge-based methods, the feature invariant approaches start at feature extraction process and face candidates finding, and later verify each candidate by spatial relations among these features, while the knowledge-based methods usually exploit information of the whole image and are sensitive to complicated backgrounds and other factors. Readers could find more works in [4][6][9]. Face detection based on color information, random labeled graph matching fall in this category.

- **` Template matching methods**

In this category, several standard patterns of a face are stored to describe the face as a whole or the facial feature separately. The correlations between an input image and the stored pattern are computed for detection. These methods have been used for both face localization and detection. Deformable template matching [2] falls in this category, where the template of faces is deformable according to some defined rules and constraints.

- **Appearance-based methods**

In contrast to template matching, the models (or templates) are learned from a set of training images, which should capture the representative variability of facial appearance. These learned models are then used for detection. More significant techniques are included in [2][3]. Examples of such type of methods are view-based face detection, Haar features and the Adaboost algorithm.

5. APPLICATIONS OF FACE RECOGNITION TECHNOLOGY

In order to prevent the frauds of ATM, it is recommended to prepare the database of all ATM customers with the banks & deployment of high resolution camera and face recognition software at all ATMs. So, whenever user will enter in ATM his photograph will be taken to permit the access after it is being matched with stored photo from the database [10].

Duplicate voter are being reported. To prevent this, a database of all voters, of course, of all constituencies, is recommended to be prepared. Then at the time of voting the resolution camera and face recognition equipped of voting site will accept a subject face 100% and generates the recognition for voting if match is found [10].

Passport and visa verification can also be done using face recognition technology.

Driving license verification can also be exercised face recognition technology.

To identify and verify terrorists at airports, railway stations and malls the face recognition technology will be the best choice as compared with other biometric technologies since other technologies cannot be helpful in crowdie places.

In defense ministry and all other important places the face technology can be deployed for better security.

This technology can also be used effectively in various important

Examinations such as SSC, HSC, Medical, Engineering, MCA, MBA, B- Pharmacy, Nursing courses etc. The examinee can be identified and verified using Face Recognition Technique.

1. In all government and private offices this system can be deployed for identification, verification and attendance.
2. It can also be deployed in police station to identify and verify the criminals.

6. CONCLUSION

Face recognition is a both challenging and important recognition technique. In this paper, we have covered a detail discussion on the various stages of a face recognition system and a brief of the different algorithms used in face recognition. Also, some popular well-known face detection techniques are described very briefly. Recently, face detection techniques have been employed in different area of applications such as face recognition, facial feature extraction, detection of facial expression, which are also the subjects to be focused of this paper. Also you can justify the face expression so you can give the various opinions on this faces.

REFRENCES

[1] .Subrat Kumar Rath, Siddharth SwarupRautaray, "A Survey on Face Detection and Recognition Techniques in Different Application Domain",

[2]. Mrs. Sunita Roy and Mr. SusantaPodder, "Face detection and its applications", IJREAT International Journal of Research in Engineering & Advanced Technology, ISSN: 2320 – 8791, Volume 1, Issue 2, April-May, 2013.

[3] .Subrat Kumar Rath, SiddharthSwarupRautaray, "A Survey on Face Detection and Recognition Techniques in Different Application Domain", I.J. Modern Education and Computer Science, 2014, 8,

34-44,Published Online August 2014 in MECS (http://www.mecs-press.org/).

[4] .K. Sobottka and I. Pitas, "Face localization and feature extraction based on shape and color information,"Proc. IEEEInt˝l Conf. Image Processing, pp. 483-486, 1996.

[5] .Al-atrash, Shady S. "Robust Face Recognition." (2011).

[6] .C. Lin, K.C. Fan, "Human face detection using geometric triangle relationship," Proc. 15th ICPR, pp. 945–948, 2000.

[7] .C. Kotropoulos and I. Pitas, "Rule-based face detection in frontal views," Proc. Int˝l Conf. Acoustics, Speech and Signal Processing, vol. 4, pp. 2537-2540, 1997.

[8] .KandlaArora, "Real Time Application of Face Recognition", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-2, Issue-5, November 2012.

[9]. E. Hjelmas and B. K. Low, "Face detection: A survey," Computer Vision and Image Understanding, vol. 83, pp.236–274, 2001.

[10] AnkurBansal, MukeshAgarwal, Anima Sharma, Anindya Gupta, "A Review Paper on FACIAL RECOGNITION", International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), Volume: 1, Issue: 4, page no. 224 – 228

[11] .http://www.cs.technion.ac.il/~ron/PAPERS/BroBroKimIJCV05.pdf

[12]. Mr. Rahul D. Dhotkar, Mr. Prakash R. Chandore, Dr. Prashant N. Chatur, "Face recognition techniques and its application", International Journal of Application or Innovation in Engineering & Management (IJAIEM), ISSN 2319 – 4847, Volume 3, Issue 3, March 2014.

[13]. Renu Bhatia, "Biometrics and Face Recognition Techniques", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCS),ISSN: 2277 128X,Volume 3, Issue 5, May 2013.

[14]. Zhang, Cha, and Zhengyou Zhang, "A survey of recent advances in face detection. Tech. rep., Microsoft Research, (2010).

[15] .N. Bhoi, M. Narayan Mohanty "Template Matching based Eye Detection in Facial Image" International Journal of Computer Applications (0975 – 8887) Volume 12– No.5, December 2010

Adaptive Routing Algorithm in MANET with Sleep Mode

Shanoo Agarwal, Anil Rao, Rohit Singhal

[1]M.Tech Scholar, [2]Associate Professor, [3]Associate Professor

Department of Computer Science, Institute of Engineering & Technology, Alwar, Rajasthan

Abstract

An ad hoc network is a group of mobile wireless nodes that collectively form a network among themselves without any permanent infrastructure. It is a challenging environment because every node operates on limited battery resource and multihop routing paths are used over constantly changing network environments due to node mobility. The primary goal of ad hoc networks is to describe for the energy-restricted protocols. Energy consumption estimation methodology is introduced for the protocol in different mobile network. Gradually, power consumption within ad hoc networks is becoming a core concern for these low-power mobile devices. This paper focuses on a different approach for energy saving within the AODV routing protocol of the ad hoc network. A wireless Ad-hoc network in sleep mode consumes less power than in idle mode, but no packets can be sent or received while in sleep mode. In this paper, we propose an Energy based Ad-Hoc on-Demand Routing algorithm that balances energy among nodes so that a minimum energy level is maintained among nodes and the life of network is increased. We focused

On increasing the extensive existence of node in the network. In our proposed work we set the minimum energy threshold limit of a mobile node, when a node reached up to the threshold limit the node goes to sleep mode, save energy and join in the event as long as possible. The research papers are published to improve the network lifetime on the network layer. Performance valuation of these strategies show a substantial reduction in power usage, with only a slightly decrease in performance. We use NS-2.34 to simulate both the AODV and AODV-Sleep under the similar scenario. We also compared and analyzed the simulation results with a popular on-demand routing protocol AODV to show the usefulness of our algorithm. From our simulations we find that the overall MANET's efficiency is enhanced.

Keywords

Mobile Ad-Hoc Networks, AODV routing protocols, Energy utilization, Sleep mode, Mobility models, Simulation analysis.

1. Introduction

Mobile Ad Hoc Networks (MANETs) correspond to the decentralized paradigms where clients themselves maintain the network in the absence of a significant infrastructure. MANET does not operate under predetermined topology means they are self-organizing, self-managing, and self-remedial type of network and the consumption of energy in mobile devices is recognized as an important issue for further research. IN MANET, Each node in the ad hoc network forwards packets for other nodes, to allow nodes to communicate are those not in direct wireless transmission range. Each mobile node function as both a router and a terminal node which is a source or destination, thus the failure of some nodes operation can greatly hinder the performance of the network and also affect the basic ease of access to the network. Since the mobile nodes in MANET have limited battery power, so it is essential to proficiently use energy of every node in MANET. The network interface hardware at a node can operate in four different modes:

Transmit mode: The mode at a node when transmitting a packet.
Receive mode: The mode at a node when receiving a packet.
Idle mode: The mode used at a node when the node is neither transmitting nor receiving a packet. This mode utilize power because the node is in listening state in wireless medium continuously to detect a packet that it should receive, so that the node can change their mode into receive mode.
Sleep mode: Sleep mode has very low power consumption than idle mode. The network interface at a node in sleep mode can neither transmit nor receive packets even node not in listening state; the network interface must be woken up to idle mode first by an explicit instruction from the node.
Energy exhaustion of nodes has been one of the main impairment to the connectivity of MANET. To evaluate the energy consumption the numerous MANET routing protocols have been built up for network.

The paper is organized as follows. Section II survey the related work to estimation of energy based Ad hoc routing protocols for MANET. Section III briefly describes the

idea and procedure of AODV routing protocols which improve the energy efficiency of MANET. Section IV introduces the design of the byte-based energy utilization method. Section V makes the energy consumption measurement under our proposed mobility models. Section VI draws the conclusion of the paper.

2. Related Work

As we know that energy consumption is one of the major issues in MANET so, already many of the work has been already performed on this. The various existing methods for appraisal of network lifetime in MANET. Several routing algorithms use the link lifetime as well as the nodes battery life time as routing metrics to allow the most consistent and energy efficient route to be selected for data transmission.

Feeney [5] shows the requirement and actual measured current represented by one popular wireless network interface card in the four possible modes. Receive and idle mode require same power, and transmit mode requires a little greater power. Sleep mode requires less power than idle mode. These measurements demonstrate that the network interface expends similar energy, whether it is simply listening or receiving data. Hence, cleverly switching to sleep mode whenever possible will significantly increase energy savings. The full version of these protocols is available from the thesis [6].

Zorzi and Rao [7]-[8] presented a routing protocol where each node follows the duty cycle that is distinct nodes wake up and sleep.

Minimum Battery Cost Routing (MBCR) has been proposed in [9]. MBCR routing protocol calculates the sum of the enduring power of all nodes in a path and uses it for choosing a path, but the method may choose a path in which there may present mobile nodes with less power. Thus, these low power mobile nodes may affect path breakage.

Syropoulos et al [10], have accomplish the use of Directional Antennas for energy efficient communication in ad hoc networks.

Jin-Man Kim et al., [11] introduced an Energy Mean Value algorithm to increase AODV routing protocol and to improve the network lifetime of MANET.

Krishna Cheong Lau and Joseph H. Kang [12] the idea to increase energy efficiency, nodes in the network goes into a sleep mode and wake up at preset time slot(s) to snoop for transmissions from its instant neighbors. The knowledge of awakening slots for neighboring nodes is used to arrange the transmissions within the neighborhood. Lastly, nodes adjust their sleeping cycles based on neighbor topology and residual battery life in order to maximize the network lifetime also satisfying the latency requirements of sensor applications.

In [13] authors have proposed a protocol named RPAR which design was based on considering the substitution between energy efficiency and latency. The participating nodes required to uphold an information table related to its neighbors. Attainment and maintenance of such information requires considerable exchange of information through beacon signals which contain lot of energy consumption hence energy efficiency is relinquish.

3. Proposed Work

We have to concentrate on the link lifetime and the energy information as routing metrics to enhance the route selection procedure of the routing protocol. To the best of our knowledge, this is the first work that initiates the link lifetime and the nodes' residual energy to augment the route discovery process that allows the routes that assures the link lifetime and the energy requirements. The power of a wireless node is very important factor due to limited energy sources our proposed work is based on the power reduction of a node. Each node in wireless network work as a router and play in the routing mechanism, the energy of moving node are limited. In our proposed solution we utilizes the node energy when it reaches the minimum power level called MINIMUN THRESHOLD. When the node reaches at minimum threshold level it goes into sleep mode after performing following function:

1. If the energy of neighbor node is greater than 50 then the cache updation is performed on the node and the new route is established through that node.

2. Otherwise, the node with maximum energy is chosen for cache updation then new route is established.

4. Simulation Model

For simulation of the real active behaviors of the nodes in a mobile ad hoc network we use NS-2. In simulation model, we have taken 10 nodes that are arbitrarily scattered in a area of 800m X 600m square region with 50 numbers of links. These factors are taken as the vital scenario. Energy model includes the radio range of 250m, 2Mbps of data

rate. Initial each node in network is assumed to have random energy. The power utilization during transmission and reception is 1.5 W and 1.0 W respectively. The traffic model used is CBR (Constant Bit Rate) with packet size of 512 bytes, rate 50 packets/sec and simulation time of 100s. The simulation is done with the help of NS-2 [5] and traffic model is generated using energy.tcl. Here we focus on Constant Bit Rate (CBR) sources (i.e. voice sources) and ftp sources (i.e. file transfer). The source-destination pairs are chosen erratically over the network. We also evaluated the protocol using the following performance parameters

A. Network lifetime
B. Packet delivery fraction
C. Discrepancy of node remaining energy

We adopt NS2 simulator to assess the performance of the proposed methodology we simulate and compare the traditional AODV based wireless ADHOC network with the proposed sleeping node methodology. More detail description of simulation parameter values are shown in table

Table I: Simulation Parameter

Type	Values
Channel	Channel/Wireless Channel
Radio Propagation Model	Propagation/Tworayground
Network Interface	Physical/Wirlessphy
Mac	Mac/802_11
Interface Queue	Queue/Droptail/Priqueue
Antenna	Antenna/Omniantenna
Link Layer	Ll
Interface	50
Routing Protocol	Aodv
Simulation Time	100s

5. Results

As the network load is increased all the protocols show significant reduction in the network life time. The results in fig.1 show that the packet delivery rate has been increases and packet drop rate decreases for our scheme. Our scheme consumes less energy as it uses a mechanism of sleep mode that ensures un-necessary wastage of nodes energy in network. Fig.1 clearly depicts that our scheme provides significant high network existence as compared to the traditional AODV protocol. From the result summary we can illustrate a conclusion that the proposed methodology performs well as compare to traditional AODV. But delay has been increases using the proposed methodology.
We have estimated
(i) Energy consumption due to routing packets
(ii) Routing overhead and
(iii) Delivery ratio for Comparison between AODV and AODV–sleep protocols and following results was observed. Several simulations are performed using NS2 network simulator and using parameters shown in table II. NS2 generates a name trace files observed using an AWK scripting. The performance reading involves AODV routing protocol.

Table II: Simulation Result Summary

Parameter	Original	Proposed
No. Of Nodes	10	10
Packet Send	10480	10519
Packet Receive	5185	8857
Routing Packets	389	200
Packet Delivery Fraction	49.48	84.20
End To End Delay	483.34	632.29
No. Of Packet Drop	5168	1658

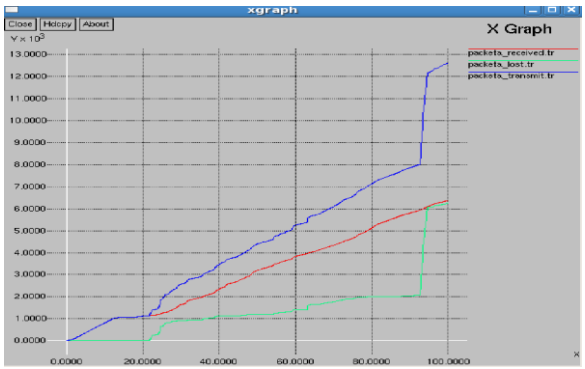


Fig 2: Result Summary of Proposed Algorithm

6. Conclusion

In this paper we propose a New-AODV protocol which improve the network lifetime in an Ad-hoc network environment and simulated in NS2. Survivability of network is improved to concern with protecting individual network nodes power. Rather directly determining the lifetime of MANET. Above all, each node's energy has a huge impact on the entire network lifetime. The proposed sleep mode scheme ensures major improvement in power aware system.

Hence, the significance of sleep mode for the systems finally depends on the wake-up time for variety of nodes. The initiation of the consciousness in the power management is proposed. In order to, recover the energy based problem and inhibit the link breakage. As a result, we know that sleep mode to AODV protocol gives noticeable result to boost the entire network lifetime.

References

[1] C. Perkins and P. Bhagwat, “Highly dynamic destination- sequenced distance-vector routing (DSDV) for mobile computers,” in ACM SIGCOMM'94 Conference on Communications Architectures, Protocols and Applications, 1994, pp. 234–244.

[2] D.B. Johnson and D.A. Maltz, “Dynamic source routing in ad hoc wireless networks,” in Mobile Computing, Imielinski and Korth, Eds. Kluwer Academic Publishers, 1996, vol. 353. pp. 153-181.

[3] C. Perkins, E. Belding-Royer and S. Das, “Ad hoc On-Demand Distance Vector (AODV) Routing,” RFC 3561 (Experimental), Jul. 2003. [Online.

[4] J. Li, D. Cordes, and J. Zhang, "Power-aware routing protocols in ad hoc wireless networks," IEEE Trans. Wireless Commun., pp. 69-81, Dec. 2005.

[5] L. Feeney and M. Nilsson.Investigating the Energy Consumption of a Wireless Network Interface in an Ad Hoc Networking Environment. In Proceedings of INFOCOM 2001, volume 3, pages 1548–1557, Anchorage, Alaska, Apr. 2001.

[6] S. PalChaudhuri. Power Mode Scheduling for Ad Hoc Network Routing. Masters Thesis, Computer Science, Rice University,May 2002.

[7] M. Zorzi and R. R. Rao."Geographic random forwarding (GeRaF) for ad hoc and sensor networks: energy and latency performance," IEEE Trans. Mobile Computing, Yol.2, No.4, pp.349-365, 2003.

[8] Singh, S., Woo, M., Raghavendra, C.S., “Power-aware routing in mobile ad hoc networks”. In: Proc. of 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking, pp. 181– 190,1998.

[9] EvangelosKranakis, Danny Krizanc and Erric Williams, Directional versus Omni Directional Antennas for Energy Consumption and k-Connectivity of Network of Sensors, October 15th 2004

Analysis of Fractal image Compression withVaryingSub-image

Vedant Rastogi,Jaspreet Kaur,Shadab Ali

[1]Associate Professor, [2]M.Tech Scholar,[3]Assistant Professor

Department of Computer Science, Institute of Engineering & Technology, Alwar, Rajasthan

Abstract

A fractal image compression partition an image in to square range blocks that are coded via self-references to other parts of the image itself. In this paper we represent a algorithm for Fractal Image Compression that covers a image with square range blocks without overlapping and introduce domain blocks D, intersect with M .Define local contractive collection of affine transformation mapping domain block D to the range block R, for each range block, a corresponding domain block and symmetry so that the domain block looks most like the part of the image then write the code in form local IFS code.

Keywords— Fractal Image Compression, Collage Theorem, iterated function system.

1. INTRODUCTION

With the ever increasing demand for images, data compression, video compression, volume visualization, sound and computer animations suffer the problem of data storage and transmission. Fractal Image Com2pression is time consuming process. Barnsley gave the concept of Fractal Image Compression in 1988. FIC uses the feature of self-similarity. This type of image representation was first proposed byBarnsley [1], Sloan [2] and Jacquin [3].In Fractal compression the image is partitioned in to image blocks called range. Each part which is range is coded by a reference to some other part of the image by transformation parameters. For high compression ratio small no of blocks are needed. Fractal image compression is time consuming process. It involves the use of fractal geometry to encode images as attractors of specific Iterative Function Systems (IFS). These IFS are taken as a set of contractive maps and contraction of an image entails finding the parameters which define them. Instead of storing exact pixel information, a compressed fractal image contains the transformations or functions needed to regenerate the image. In fractal image compression decoding process is faster than encoding process. Many exhaustive search algorithms were used to find the parameters. For encoding of any image partitioning, block wise basis through quad trees, H-V partitioning and other Triangular partition have been applied. But the problem arises to encoding with varying sub image shape. Recently, evolutionary computing based techniques are being applied to this

problem. Our algorithm provides a method for directed randomness to arrive at the optimal parameters keeping in view the compression ratio, the quality of the decoded images and the encoding or decoding time.

2. BASIC FUNDAMENTALS

A. Fractal Image Compression

Iterated Function system set the foundation for Fractal Image Compression. The basic idea of IFS is to create a finite set of contraction mapping or affine transformation based on what image one desire to create. If these mapping are contractive, applying the IFS to a seed image will eventually produce an attractor of the map. IFS compression mathematical frame work start with some target image T which lies in a sub set $S \subset \mathbb{R}^2$.The target image T is rendered on a computer graphics monitor to achieve the Fractal Image Compression, an affine transformation[9].

$$w(\mathbf{x}) = w\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} e \\ f \end{pmatrix}$$

is introduced with coefficient that produces a new image ,w1(T),with dimension smaller than that of T. This ensure a contractive mapping [5], [6]. The user adjusts the coefficients a, b, c, d, e, f in order to shrink, translate, rotate, and shear the new image, $w_1(T)$, on the screen so that it lies over a part of T. By placing the w1 (T), it is fixed and recorded to keep controlling, we have new affine transformation $w_2(T)$ introduced along with its sub copy T. This process is carried out with new image as was done previous one. Overlaps must be avoided between images. Theorem Overlaps only complicate the situation, although there exist compression methods, such as wavelets, which confront this issue. In this manner, a set of affine transformations $w_1, w_2, w_3 \square , w_n$ is obtained such that $\tilde{T} = \bigsqcup_{n=1}^{N} w_n(T)$ Where N is small no, Collage theorem assurethat attractor A is very near to T . If T =T then A=T that isA is very close T and make it resolution independent We adjusted the parameter of transformation for controlling the attractor of the IFS and this is called fractal image compression images can be built up using Fractal Image Compression by working on subsets of the image, where each subset is represented by an

IFS. Increasing the number of coefficients used,the size of the digital file increases. Thus, it is optimal to find as few affine transformations as possible to represent an image [7], [9].

B The Collage Theorem

We take a complete metric space (X, d). Let $T \in H(\mathrm{X})$ be given, and let $\varepsilon \geq 0$ be given. We have taken IFS $\{\mathrm{X}; (w_0), w_1, w_2, ..., w_N\}$ withcontractivityfactor $0 \leq s < 1$ so that $h\left(T, \prod_{n=1}^{N} w_n(T)\right) \leq \varepsilon$, Where h(d) is theHausdorffmetric. The $h(T, A) \leq \frac{\varepsilon}{1-s}$, where A is the attractor of the IFS.

$$h(T, A) \leq (1-s)^{-1} h\left(T, \prod_{n=1}^{N} w_n(T)\right)$$

Equivalently, for all $T \in H(\mathrm{X})$ [2].The Collage Theorem tells us that in order to find IFS whose attractor looks like a given set, we must find a set of contractive transformations on a suitable space, in which the given set lies, so that the distance between the given set and the union of the transformations is small. In other words, the union of the transformations is close to, or looks like, the given set. The IFS which satisfies this may be a good candidate for reproducing the given set, or image, by the attractor of the IFS. Thus this image can be stored using much less space.

C The Fractal Transform Theory

Fractal transform theory is the theory about local IFS. Local IFS does complicate the theory of fractal image compression while in practice it is simplifying the process. A global transformation on a space X is a transformation, which is defined on all points in X; whereas, a local transformation is one whose domain is a subset of the space X and the transformation need not act on all points in X. It is convenient to allow an IFS to act upon domains that are subsets of the space, rather it act upon whole Domain. This is called a local IFS. It is to find subspaces (or sub-images) of the original image space, which can be regenerated using an IFS. Where possible, if one IFS can be used in place of several IFS's which reproduce similar sub-images, it is more efficient in terms of storage space to use that one IFS. It is more likely that an image will require more than one IFS to reproduce a compressed image, which closely resembles the original.

Let (X, d) be a compact metric space. Let R be a nonempty subset of X. Let $w: R \to \mathrm{X}$ and let s be a real number with $0 \leq s < 1$.If $d(w(x), w(y)) \leq (s)(d(x, y)) \ \forall x, y \in R$ then w is called a local contraction mapping on (X, d).The number s is a contractility factor for w [2].

3. PREVIOUS WORK

In this section, we give a survey of the partitioning methods for fractal compression. The most basic class of partitions for fractal image compression are uniform partitions, by which we denote a partition consisting of square atomic blocks of size pixels. Uniform partitions of other types can be defined by a regular tiling of the plane, but are rarely used for fractal image compression [8]. For a uniform partition based on square atomic blocks the block size has to be specified; apart from those uniform partitions are image-independent[14],[15].

A. Quad tree partition approach

In this quad tree based fractal coders have been presented. In this whole image is presented as a single range, this range is splits in to four quadrants. A quad tree portions is a representation of an image as a tree. Each node, corresponding to a square portion of the image, contains four sub nodes. The squares at the nodes are compared with domains from the domain pool, which are twice the range size. The pixels in the domain are averaged in groups of four so that the domain is reduced to the size of the range, and the affine transformation of the pixel values is found that minimizes the rms difference between the transformed domain pixel values and the range pixel values. All the potential domains are compared with a range. If the resulting optimal rms value is above a preselected threshold and if the depth of the quad tree is less than a preselected maximum depth, then the range square is subdivided into four quadrants and the process is repeated. If the rms value is below the threshold, the optimal domain and affine transformation on pixel values are stored. A quad tree partition algorithm initially partitions the image into a set of large range blocks. A corresponding set of domain block is constructed [9]. Using a distance metric, the domain pool is searched repeatedly to find the best possible transformation for every range. The best transformation is stored and range block is said to be covered. If the distance between the best domain and a range block is less than the user- specified acceptable threshold. If the best transformation is discarded, the process is repeated after partitioning [14].

B. JPEG Compression Techniques

JPEG is a lossy compression for photographic images. Degree of compression in JPEG compression can be adjusted and allow a selected tradeoff between storage size and image quality. It has 10:1 compression ratio. It is the most common format for storing and transmitting photographic image on the World Wide Web. It is best on photographs and painting used by realistic scene with smooth variation of tone and color. It is very popular for web usage. On the other hand JPEG is not well suited for line drawing and other textual or iconic graphics, where the sharp contrast between adjacent pixel cause noticeable artifacts. JPEG is also not well suited to files that will undergo multiple edits.

C. Discrete Cosine Transform

A discrete Cosine transform (DCT) expresses a sequence of finitely many data points in term of a sum of cosine function oscillating at different frequencies. DCTs are important to numerous applications in science and engineering, from lossy compression of audio and images, where small high-frequency components can be discarded the use of cosine function in compression are much more efficient. DCT is a Fourier-related transform similar to the Discrete Fourier Transform (DFT), but using only real numbers. DCTs are equivalent to DFTs of roughly twice the length operating on real data with even symmetry [10].

D. Delta Compression

Delta Compression was a simply early approach of reducing the number of bits .That method of data compression, along with other early lossless method of data compression was an attempt to transmit images of space collected from space problems [11]. Because of low power transmitter, the communication bandwidth did not allow image to send. The concept of Delta Compression is to take the difference in neighboring pixel values. The average change in pixel values is small from one pixel to next. This guarantees that after the Delta Compression has been applied, the magnitudes of the differences are smaller than the original pixel values. Thus, a smaller number of bits per pixel are required to store the image.

E. Periodic functions

A function $f(t)$ is called periodic if there exists a constant T > 0 for which $f(t+T)=f(t),$ for any t in the domain of definition of $f(t)$, where t and t + T lie in this domain. The smallest such T is called the period of $f(t)$ [13]. There are many periodic function. If we were to plot a periodic function on some interval $a \le t \le a+T$, we would obtain the entire graph by periodic repetition of the portion of the graph corresponding to $a \le t \le a+T$ [13]. If T is the period of $f(t)$, then any integer multiple of T, say kT, where k is any positive integer, is also a period of $f(t)$ [13].

F. Fourier Transform

Fourier Transform is to determine and work with the spatial frequency content of an image. Images are two dimensional discrete finite signals and we represent it by Fourier transform of a two-dimensional signal has a matrix representation and contains the amplitudes of the fundamental frequencies that make up. Each component of Fourier transformindicates the strength of a particular frequency. Applying Fourier transformation to an image and achieve compression of the image, it is necessary to quantize it. Quantizing is a rounding procedure in which the high frequencies are omitted. Ideally, many entries in the matrix will be set to zero. By doing this, less storage space is needed to represent the image. The image is decompressed by application of the inverse transform. The resulting image matrix will have values close to the corresponding entries in the original image. This is how it is possible for the new image to resemble the original image.

4. FRACTAL TRANSFORM THEORY

Fractal transform theory is the theory of local IFS. Although local IFS do complicate the theory of fractal image compression, in practice it simplifies the process. A global transformation on a space X is a transformation, which is defined on all points in X, whereas, a local transformation is one whose domain is a subset of the space X and the transformation need not act on all points in X .Rather than allowing an IFS to act upon only on the whole domain, it is convenient to allow an IFS to act upon domains that are subsets of the space. This type of IFS is called local IFS. The idea of fractal image compression, is to find subspaces or sub-images of the original image space, which can be regenerated using an IFS. Where possible, if one IFS can be used in place of several IFS's which reproduce similar sub-images, it is more efficient in terms of storage space to use that one IFS. It is more likely that an image will require more than one IFS to reproduce a compressed image, which closely resembles the original. Let (X,d) be a compact metric space. Let R be a nonempty subset of X. Let $w: R \to X$ and let s be a real number with $0 \le s < 1$, $d(w(x),w(y)) \le (s)(d(x,y)) \ \forall x,y \in R$ w is called a local contraction mapping on (X,d). The number s is a

contractivity factor for w [2]. Let (X, d) be a compact metric space, and local contraction mapping $w_i : R_i \to \mathrm{X}_{\mathrm{w}}(\mathrm{X}, d)$ with N is positive integer and contractivity factor s_i fori=1, 2…N, then $\{w_i : R_i \to \mathrm{X} : i = 1,2,..., N\}$ is called local IFS $s = \max\{s_i : i = 1,2,\square\ N\}$ is called the contractivity factor of the local IFS [2].If we let S denote the set of all subsets of X, then we can define the operator $W_{local} : S \to S$ according to [2]. Under certain restraints, W_{local} can be defined as contractive on certain subsets of the Hausdorffspace. This allows us to create a fractal compression system. If A is a nonempty subset of X, we call Aan attractor of the local IFS if $W_{local}(A) = A$. If A and B are attractors, then so is $A \cup B$. If there is an attractor, there is a largest attractor, which is the one that contains all the other attractors. This largest attractor is referred to as the attractor of W_{local} and is found by taking the union of all the other attractors in W_{local} [2]. If we define an IFS to be $\{w_i : R_i \to \mathrm{X} : i = 1,2,\square\ ,N\}$ and we suppose that the sets R_i are compact, then we can define a sequence of compact subsets of X by [2] ,if $A_0 = \mathrm{X}$, then $A_n = \bigcup_{i=1}^{N} w_i(R_i \cap A_{n-1})$ for n=1,2,3,… Because the IFS consists of contractive mappings, such that $A_o \supset A_1 \supset A_2 \supset A_3 \supset \square$. So, A_n is a decreasing sequence of compact sets.There exists a compact set $A \subset \mathrm{X}$ so that $\lim_{n\to\infty} A_n = A$ & $A = \bigcup_{i=1}^{N} w_i(R_i \cap A) = W_{local}(A)$.As mentioned before, if A is not empty, then A is the maximal attractor for the local IFS. If one can find a compact set B such that $W_{local}(B) \supset B$, then the possibility that A is empty is ruled out. A corresponds to the attractor of an IFS in a fractal image compression scheme. The coefficients of the mappings w_i are crucial in the determination of the compression of an image. A represents what the image would look like after applying the mappings to subsets of the image.

5. FRACTAL IMAGE COMPRESSION ENHANCED ALGORITHM

We will propose an algorithm which increases the compression ratio. Fractal Image Compression could be described as a transformation space algorithm first generates uniformly block-based transformation then its space is remove to reduce the no of transformation.

1) Input a binary image, call it M.

2) Cover M with square range blocks. The total set of range blocks must cover M, without overlapping.

3) Introduce the domain blocks D, they must intersect with M. The sides of the domain blocks are twice the sides of the range blocks.

4) Define a collection of local contractive affine transformations mapping domain block D to the range block R_i.

5) For each range block, choose a corresponding domain block and symmetry so that the domain block looks most like the part of the image in the range block.

6) Write out the compressed data in the form of a local IFS code.

Apply a lossless data compression algorithm to obtain a compressed IFS code. In practice these steps can be carried out on a digital image. The compression isattained by storing the coefficients of the transformations, rather than storing the image pixel by pixel. In this section we represent coding results obtain by our fractal image compression

5. Summary and Conclusion

Fractal image compression is a method to compress an image and achieve doubling the compression ratio. This paper proposed a algorithm to compress an image block based varying sub image. The time taken for it is about half in processing as it compare to traditional block based algorithm. In block based searching, exhaustive searching is done to find out the starting point and take the most time of searching. While this algorithm do exhaustive search to find out first seed block in each region It shows that the time taken to extend each region is relatively small, which results in a faster encoding time than block-based system.

REFERENCES

[1] M. F. Barnsley and A. D. Sloan, "Chaotic compression"Comput.Graph. World, Nov. 1987

[2] M.F. BARNSLEY, A.D. SLOAN, "A better way to compress images", BYTE, Jan1988, p.215-223.

[3] A. E. Jacquin, "A fractal theory of iterated Markov operators with applications to digital image coding**,"**Ph.D.Dissertation, Georgia Inst. Technol., Atlanta, Aug.1989

[4] A. E. Jacquin, "Image coding based on a fractal theory of iterated contractive image transformations," IEEE Trans. Image Processing, vol. 1, pp. 18–30, Jan.

[5] Barnsley, M.(1988) Fractals Everywhere, Academic Press, San Diego

[6] Kaouri, A. H. .Fractal coding of still images.Queen's university ofBelfast, UK. 2002.

[7] Barnsley, Michael and Lyman P. Hurd; Fractal Image Compression, AK Peters, Ltd., 1993.

[8] F. Mendivil, "The application of a fast nonseperable discrete periodic wavelet transform to fractal imageCompression," in Proc. Fractals Eng., Delft, the Netherlands, 1999.

[9] Chaurasia, V. and Somkuwar, A. Speed up Technique for Fractal Image Compression, 2009.

[10] Tsai, M.J.,Villasenor , J. D., and Chen , F. stack –Run Image Coding , IEEE Trans.CSVT , vol.6 no. 5, Oct 1996,pp. 519-521.

[11] Russ, John C.; the Image Processing Handbook, CRCPress, 1994.

[12] Darrel Hankerson, Greg A. Harris, Peter D. Johnson, Jr., Introduction to Information Theory andData Compression, CRC Press.

[13] Tolstoy, Georgie P.; Fourier series, Dover Publications, 1976.

[14] R. Pan and s. J. Reeves, "efficient huber-markov edge Preserving image restoration," IEE Trans. ImageProcess. vol. 15, no. 12, pp. 3728– 3735, Dec. 2006.

[15] Zhao, E. and Liu, D. Fractal Image Compression Methods: A Review. International Conference on Information Technology and Applications. 2005

Analysis of RIP, EIGRP and OSPF Routing Protocol

Deepak Choudhary[1],Anil Rao[2],Alok Ranjan Vashishtha
[1]Assistant Professor, [2]Assistant Professor,[3]
Department of Computer Science, Institute of Engineering & Technology, Alwar, Rajasthan

Abstract

Performance of a network is based on routing protocols. RIPv1, RIPv2, EIGRP and OSPF are the dynamic routing protocols being used in the practical networks to propagate network topology information to the neighboring routers. There are different classes of routing protocols, two of which are Exterior Gateway Protocol (EGP) and Interior Gateway Protocol (IGP). A routing protocol can be dynamic or static, as well as distance-vector or link-state. In this report, we will focus on Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and Enhanced Interior Gateway Routing Protocol (EIGRP). All three protocols are dynamic IGPs, meaning that these protocols route packets within one Autonomous System (AS). RIP is a distance-vector protocol; EIGRP is an enhanced distance vector protocol developed by Cisco and OSPF is a link-state routing protocol. In this research work I will analyze the performance of these protocols in term of their convergence, traffic, CPU utilization by changing special parameters within network. OPNET simulation tool is a standard tools used to design the network and analysis of the results. I will study characteristics such as convergence time and routing traffic sent within small and large topologies. Using OPNET or Packet Tracer, I will compare performance in order to determine the best routing protocol for a given network topology.

Keywords-Interior Gateway Protocol (IGP), Exterior Gateway Protocol (EGP), Link State Routing Protocols (LSRP), Distance Vector Routing Protocols (DVRP), Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OPSF).

1. INTRODUCTION

Communication is a method of sharing information to each other for transferring packet between two nodes. Communication is directly between nodes or through intermediate nodes acting as routers. In a petite time mankind developed a rules and languages to communicate with each other. Combination of these rules and languages are called protocols. Most important aspect of communication is routing and routing is done by routing protocols. Routing protocols specify how routers communicate with each other by disseminating information. The router has prior knowledge about the adjacent networks which can assist in selecting the routes between two nodes. There are different types of routing protocols in the IP networks. Three classes are common on IP networks as follows:

1) Interior gateway routing over link state routing protocols, such as IS-IS and OSPF.

2) Interior gateway routing over distance vector protocols, such as RIP, IGRP and EIGRP.

3) Exterior gateway routing, such as BGP v4 routing protocol.

Routing protocols define the path of each packet from source to destination. To complete this task, routers use routing tables, which contain information about possible destinations in the network and the metrics (distance, cost, bandwidth, etc.) to these destinations. Routers have information regarding the neighbor routers around them. In a network topology for forwarding packets various routing protocols are being used. Routers maintain a routing table for successful delivery of the packets from the source node to the correct destined node. The extent of information stored by a router about the network depends on the algorithm it follows. Most of the popular routing algorithms used are RIP, OSPF, IGRP and EIGRP.A routing protocol works based on an algorithm. Routing algorithm also based on metrics to find the path to transmit data across two networks. Metrics also include cost, bandwidth, Maximum Transmit Unit, delay, number of hop count these metrics also save or store in routing table.

Routing protocol has two types. First one is an interior gate way protocol and other one is an exterior gateway protocol. OSPF is also interior gate way protocol, other interior gate way Protocol are RIP, EIGRP, IGRP. BGP is Exterior gate way protocol. CHARACTERSTICS OF ROUTING PROTOCOLS

The characteristics of routing protocols are:

Convergence: The time needed for all routers in the network should be small so that the routing specific information can be easily known.

Loop Free: The routing protocol should ensure a loop free route. The advantage of using, such routes are to efficiently obtain the available bandwidth.

Best Routes: The routing protocol selects the best path to the destination network.

Security: The protocol ensures a secured transmission of the data to a given destination.

METRICS AND ROUTING

Metrics

The measurements of path cost usually depend on the metric parameters. Metrics are used in a routing protocol to decide which path to use to transmit a packet through an internetwork.

Purpose of a Metric

A metric is defined as a value utilized by the routing protocols, which is used to allocate a cost for reaching the destination. Metrics determine the best path in case of multiple paths present in the same destination. There are different ways to calculate metrics for each routing protocol. For instance, OSPF uses bandwidth while RIP (Routing Information Protocol) uses hop count and EIGRP uses a combination of bandwidth and delay.

Metric Parameters

A metric is measured to select the routes as a mean of ranking them from most preferred to least preferred. Different metrics are used by different routing protocols. In IP routing protocols, the following metrics are used mostly:

Hop count: It counts the number of routers for which a packet traverses in order to reach the destination.

Bandwidth: A bandwidth metric choose its path based on bandwidth speed thus preferring high bandwidth link over low bandwidth.

Delay: Delay is a measure of the time for a packet to pass through a path. Delay depends on some factors, such as link bandwidth, utilization, physical distance traveled and port queues.

Cost: The network administrator or Internet Operating System (IOS) estimates the cost to specify an ideal route. The cost can be represented either as a metric or a combination of metrics.

Load: It is described as the traffic utilization of a defined link. The routingProtocol use load in the calculation of a best route.

Reliability: It calculates the link failure probability and it can be calculated from earlier failures or interface error count.

2. CLASSIFICATION OF ROUTING PROTOCOLS

The classifications of routing protocols are:

Static and dynamic routing protocols

Classfuland Classless routing protocols

Distance Vector and Link State routing protocols.

Static versus Dynamic Routing:

Static routing is a routing process whose routing table follows a manual construction and fixed routes at boot time. The routing table needs to be updated by the network administrator when a new network is added and discarded in the AS. Static routing is mainly used for small networks. Its performance degrades when the network topology is changed routing. It usually provides more control for the system administration. In static routing, the network has more control over the network. Its simple functionality and less CPU processing time are also an advantage but poor performance experienced when network topology changes, complexity of reconfiguring network topology changes and difficult manual setup procedure are still major drawbacks of static routing. On the contrary, dynamic routing is a routing protocol in which the routing tables are formed automatically such that the neighboring routers exchange messages with each other. The best route procedure is conducted based on bandwidth, link cost, hop number and delay. The protocol usually updates these values. Dynamic

routing protocol has the advantage of shorter time spent by the administrator in maintaining and configuring routes. However it has diversity problems like routing loops and route inconsistency.

Classful and Classless Routing Protocols:

Based on the subnet mask, routing protocols are divided into Classful and Classless routing as below:

Table 1: Classification of Routing Protocols

Distance Vector	Link State	Class
RIP, IGRP		Classful
RIPv2, EIGRP	OSPF,IS-IS,NLSP	Classless

Classful Routing

In Classful routing, subnet masks perform the same functionality all through the network topology and this kind of protocol does not send information of the subnet mask. If a router calculates a route, it will perform the following functions.

Classless Routing

In classless routing, the subnet mask can be changed in network topology and routing updates are included. Most networks do not depend on classes for being allocated these days and also for determining the subnet mask, the value of the first octet is not used. Classless routing protocols support non adjacent networks.

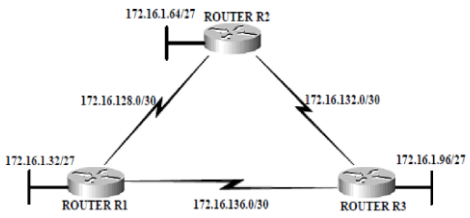


Fig: Classless routing with different subnet mask

Link State and Distance Vector Routing:

Link State Routing

Link State Routing (LSR) protocols are also known as Shortest Path First (SPF) protocol where the function of each router is to determine the shortest path among the network. Each router maintains a database called link state database. The Link State Advertisements (LSA) is responsible for exchanging the routing information among the nodes. These databases provide information of the link cost in the network and then a routing table is formed. This routing table carries information about the forwarded packets and also indicates the set of paths and their link cost. Dijkstra algorithm is used for calculating the path and cost for each link. The link cost is set by the network operator and it is represented as the weight or length of that particular link. The load balancing performance is achieved after assigning the link cost. Thus link congestion of the network resources can be evaded. Therefore, a network operator can change the routing by varying the link cost. Link state protocols make better routing decision and minimize overall broadcast traffic and are able to make a better routing decision. Two of the most common types of LSR protocols are OSPF and IS-IS. OSPF determines the shortest distance between nodes based on the weight of the link.

OSPF [Open Shortest Path First]

OSPF uses a link state routing algorithm that operates within a single AS. OSPF is an efficient IGP and may exhibit faster routing compared to RIP. OSPF maintains the routing table for all connections in the network while RIP only maintains the routing table of the best path for every destination. Each OSPF router stores the local network connection state with Link State Advertisement (LSA) and advertises to the entire AS. Each router receives the LSA generated by all routers within the AS. Each LSA is the description of the surrounding network topology of a router. When a new router is added to the network, it will broadcast hello messages to every neighbor and will receive the feedback hello messages from its neighbors. Eventually, routers establish connections with newly added router and synchronize their routing databases. Every router broadcasts link state update messages when network topology changes. Consequently, all routers may keep same information of network topology. Every router calculates the best paths to all destinations and indicates the closet router for each transmission. OSPF is the most widely used IGP in large enterprise networks. Open Shortest Path First is an open standard routing protocol. It is the successor of RIP routing protocol. It is a classless

routing protocol. It works with link state advertisement and uses Dijkstra algorithm to find the shortest path.

Distance Vector Routing

Distance vector routing protocol presents routes as a function of distance and direction vectors where the distance is represented as hop count metrics and direction is represented as exit interface. In DVR, for each destination, a specific distance vector is maintained for all the nodes used in the network. The distance vector comprises of destination ID, shortest distance and next hop. Here each node passes a distance vector to its neighbor and informs about the shortest paths. Thus they discover routes coming from the adjacent nodes and advertise those routes from their own side. Each node depends on its neighboring nodes for collecting the route information. The nodes are responsible for exchanging the distance vector and the time needed for this purpose can vary from 10 to 90 seconds.

Distance vector routing protocol uses the BellmanFord algorithm for identifying the best path. For calculating the best network path, different methods are used by the Distance Vector (DV) routing protocols. But, for all DV routing protocols, the main characteristic of such algorithms is found to be same. For identifying the best path in a network, various route metrics are used to calculate the direction and the distance. For example- EIGRP uses the diffusion update algorithm (DUAL) for calculating the cost which is needed to reach a destination. Routing Information Protocol (RIP) uses hop count for choosing the best path and IGRP determines the best path by taking information of delay and bandwidth availability.

RIP [Routing Information Protocol]

RIP is a distance vectored routing protocols & class-full routing protocol where updates are exchanged through broadcast. The routing table is exchanged every 30 seconds among the routers in the inter-network. The RIP protocol uses hop count as the metric to find the shortest path but the maximum allowable hop count is 15 by default. The RIP protocols is used only for a small network and is ineffective for a large network. The Administrative Distance of RIP is 120. RIP is a distance vector dynamic routing protocol that employs the hop count as a routing metric. RIP is implemented on top ofthe User Datagram Protocol (UDP) as its transport protocol. It is assigned the reserved port number 520. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. RIP selects paths that have the smallest hop counts. However, the path may be the slowest in the network. RIP is simple and efficient in small networks. However, it may be inefficient in larger networks. Each router updates its own routing table by communicating with neighboring routers. RIP has lower power consumption and memory than some other routing protocols. RIP may be implemented in all types of routing devices. Consequently, it is a better choice in a multiband, mixed network.

Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP is a Cisco proprietary routing protocol hence, a network with a non-Cisco router cannot deploy EIGRP. It is based on a new route calculation algorithm called the Diffusing Update Algorithm (DUAL). It has features of both distance vector and link state protocols. EIGRP metrics are based on reliability, MTU, delay, load, and bandwidth. Delay and bandwidth are the basic parameters for calculating metrics. EIGRP collects data from three tables. The first is the neighbors table, which stores data about neighboring routers that are directly accessible through interfaces that are connected. The second is the topology table, which contains the aggregation of the routing tables that are gathered from all neighbors that are directly connected. It contains a list of destination networks in the EIGRP routed network and their respective metrics. The third routing table stores the actual routes to all destinations. EIGRP differs from most distance vector protocols because it does not rely on periodic route dumps. Hence, it is capable of maintaining its topology table. Information that is to be routed is only exchanged when the new neighbors adjacencies is established. The EIGRP router maintains its own routing table and tables of its neighbors.

3. LITERATURE SURVEY

This Content demonstrates previous examined work related to this research topic -

C.Mahendran & N.Nazumudeen analyzed in this paper, they propose the idea of routing protocols, starting with an overview of the basics of Interior Gateway Protocols (IGP). And also describe the idea of Link State Routing Protocols (LSRP) and Distance Vector Routing Protocols (DVRP) while making a comparison which should determine the protocol needed for each network topology. According to the designed simulation experiment scenarios compare the difference between RIPv1, RIPv2, OSPF and EIGRP routing protocols. Among the IGP types the best protocol is

EIGRP because it provides a better performance than RIP and OSPF, it has a good impact in the world of networking due to its fast convergence time, improved scalability and for sure the great handling of routing loops and also EIGRP has a great impact in HTTP application which gives it the power to be in the lead of routing protocols. This paper also explained that a more variable level of delay due to network congestion. IP network delays can range from just a few milliseconds to several hundred milliseconds. EIGRP provides lowest delay and RIP provides highest delay.

TABLE 2: DIFFERENCE BETWEEN DVRP AND LSRP

Algorithms	**DVRP**	**LSRP**
Ease of configuration	Yes	No
Complexity	No	Yes
Bandwidth Consumption	High	Low

Shah A. &WaqasJ.Rana explained OSPF (Open shortest path first) and RIP (Routing information protocol) commonly used protocols in networking. During this research work, accessible the comparative study of two elected protocols OSPF and RIP. Proportional investigation conducted for real time data by using RIP and OSPF protocols within same network. Result shows that OSPF takes 13.495 seconds in convergence OSPF multi area and OSPF single area takes 12.683 seconds which approximately. Another result is RIP and RIP v2 network convergence results shows that RIPv2 is next version of RIP with some enhancements. In this paper with the help of Graph in core network convergence behavior changes inside core OSPF takes more time in convergence as compare to RIP and RIPV2 network converged faster inside core area as compare to OSPF. Comparison between OSPF convergences with RIP convergence shows that OSPF network convergence is faster as compare to RIP convergence and it is not depend that what type of network topology has been used.

Don Xu and LjiljanaTrajkovicdemonstrate in a paper that Simulation results indicate that RIP performs better in terms of voice packet delay because it is a simple routing protocol that relies on distance vector algorithms. RIP generates less protocol traffic compared to EIGRP and OSPF, especially in medium size networks simulated in this project. RIP's weakness is slower convergence time in larger networks. This weakness may cause inconsistent routing entries and occasionally results in routing loops or metrics approaching infinity. RIP is preferred in networks smaller than 15 hops.EIGRP performs better in terms of network convergence, routing traffic, and Ethernet delay.

4. CONCLUSION

Using dynamic routing is easier for the system administrator, than using labor intensive, manually achieved, static routing method but it will cost in terms of router CPU process and bandwidth in the network links. I will use OPNET as our tool to analyze and compare the performance of three routing protocols commonly used in today's networks: RIP, OSPF, and EIGRP. In the simulator OPNET, I simulate these protocols for a particular topology and find the routing table for the network. The routing table gives the shortest path to reach the destination on the basis of the protocol implemented and the metric that the routing protocol uses. I will first examine the routing tables of the small ring topology to gain a better understanding of each routing protocol's metric calculations and path routing systems. On the other hand, RIP sends full routing information through periodic updates, which floods the network and unnecessarily wastes bandwidth. In order to be able to compare the performance of the protocols, I will collect convergence and routing traffic sent statistics. In this research work I will analyze the performance of these protocols in term of their convergence, traffic, CPU utilization by changing special parameters within network. In order to be able to compare the performance of the protocols, I will do analysis which is the best choice protocol in the selected protocol for all network topologies implemented as which has a fast convergence, while also efficiently utilizing bandwidth..

REFERENCES

[1] Shah A., Waqas J. Rana, Ibrahim Group of Industries, Faisalabad, Pakistan, United Band Limited Performance "Analysis of RIP and OSPF,In Network Using OPNET" Vol. 10, Issue 6, No 2, November 2013.

[2] N. Nazumudeen, C.Mahendran, "Performance Analysis of Dynamic Routing Protocols Using Packet Tracer", IJIRSET, vol 3, Feb 2014, Department of ECE, A.C College of Engineering and Technology,Karaikudi, India.

[3] RickGraziani and Allan Jonson, "Routing protocols and concepts: CCNA Exploration companion guide" Pearson Education. London, 2008.

[4] Xu Don and LjiljanaTrajkovic (2011) "OSPF, EIGRP, and RIP Performance analysis based on OPNET", Washington, DC, Aug. 2011.

[5] Michael Valentine and Andrew Whitaker, "CCNA Third Edition "PearsonEducation. London, 2008 (ISBN: 978-81-317-2088-2)

.

Artificial Neural Networks Based Voice Recognition

Pragati Gaur[1], Nitin Sharma[2]

[1]M.Tech Scholar, [2]Assistant Professor,

Department of Computer Science, Institute of Engineering & Technology, Alwar, Rajasthan

Abstract

The synergism of Web and phone technologies has led to the development of a new innovative voice Web network. The voice Web requires a voice recognition and authentication system incorporating a reliable voice recognition technique for secure information access on the Internet. In line with this requirement, we investigate the applicability of artificial neural networks to voice recognition. Voice recognition is a process by which machine authenticates the claimed identity of a person from his or her voice characteristics .A major application area of such systems would be providing security for telephone-mediated transaction systems where some form of "biometric" identification is desirable . Due to the great potential shown by artificial neural networks (ANNs) in the field of voice recognition, we evaluate the performance of a variant of the multi-layer perception ANN in the task of speaker verification and identification. An artificial neural network, specially the probabilistic neural network model, was then employed to recognize and classify vowel signals into their respective Categories. A series of parameter settings for the PNN model was investigated and the results obtained were analyzed and discussed.

Keywords—Speech, Speaker, Artificial Neural Network (ANN), Voice Recognition, Acoustic modeling**.**

1. INTRODUCTION

The Voice recognition systems fall into two main categories, namely: speaker identification systems and speaker verification systems. In speaker identification, the goal is to identify an unknown voice from a set of known voices. Whereas, the objective of speaker verification is to verify whether an unknown voice matches the voice of a speaker whose identity is being claimed. Speaker identification systems are mainly used in criminal investigation while speaker verification systems are used in security access control. This technique makes it possible to use the speaker's voice to verify their identity and control access to services such as voice dialing, banking by telephone, telephone shopping, database access services, information services, voice mail, security control for confidential information areas, and remote access to computers .Voice recognition methods can also be divided into text-dependent and text-independent speaker recognition methods. The former require the speaker to say key words or sentences having the same text for both training and recognition trials, whereas the latter do not rely on a specific text being spoken. Both text-dependent and independent methods share a problem however. These systems can be easily deceived because someone who plays back the recorded voice of a registered speaker saying the key words or sentences can be accepted as the registered speaker. To cope with this problem, there are methods in which a small set of words, such as digits, are used as key words and each user is prompted to utter a given sequence of key words that is randomly chosen every time the system is used. Yet even this method is not completely reliable, since it can be deceived with advanced electronic recording equipment that can reproduce key words in a requested order.

Most signal processing involves processing a signal without concern for the quality or information content of that signal. In voice processing, voice is processed on a frame by-frame basis usually only with the concern that the frame is either speech or silence The usable voice frames can be defined as frames of voice that contain higher information content compared to unusable frames with reference to a particular application. We have been investigating a speaker identification system to identify usable voice frames. We then determine a method for identifying those frames as usable using a different approach. However, knowing how reliable the information is in a frame of voice can be very important and useful. This is where usable voice detection and extraction can play a very important role. The usable speech frames can be defined as frames of speech that contain higher information content compared to unusable frames with reference to a particular application. We have been investigating a speaker identification system to identify usable voice frames .We then determine a method for identifying those frames as usable using a different approach. This paper emphasizes on text dependent speaker identification, which deals with detecting a particular speaker from a known population. The system prompts the user to provide voice utterance. System identifies the user

by comparing the codebook of voice utterance with those of the stored in the database and lists, which contain the most likely speakers, could have given that speech utterance. The voice signal is recorded for N speakers further the features are extracted. Feature extraction is done by means of LPC coefficients, calculating AMDF, and DFT. The neural network is trained by applying these features as input parameters. The features are stored in templates for further comparison. The features for the speaker who has to be identified are extracted and compared with the stored templates using Back Propagation Algorithm. Here, the trained network corresponds to the output; the input is the extracted features of the speaker to be identified. The network does the weight adjustment and the best match is found to identify the speaker. The number of epochs required to get the target decides the network performance

2. APPROACHES TO VOICE RECOGNITION

There are following approaches used for voice recognition

1. The Acoustic Phonetic approach

2. The Pattern Recognition approach

3. The Artificial Intelligence approach

A. The Acoustic Phonetic Approach

The acoustic phonetic approach is based upon the theory ofacoustic phonetics that postulate that there exist a set of finite,distinctive phonetic units in spoken language and that thephonetic units are broadly characterized by a set of propertiesthat can be seen in the speech signal, the first step in this approach is called segmentation and labeling phase. It involves segmenting the speech signal into discrete (in Time) regions where the acoustic properties of the signal are representatives of one of the several phonetic units or classes and then attaching one or more phonetic labels to each segmented region according to acoustic properties. For voice recognition, a second step is required. This second step attempts to determine a valid word (or a string of words) from the sequence of phonetic labels produced in the first step, which is consistent with the constraints of the voice recognition task.

B. The Pattern Recognition Approach

The Pattern Recognition approach to speech is basically one

In which the speech patterns are used directly without explicit

Feature determination (in the acoustic – phonetic sense) and segmentation. As in most pattern recognition approaches, the method has two steps – namely, training of speech patterns, and recognition of patterns via pattern comparison. Speech is brought into a system via a training procedure The concept is that if enough versions of a pattern to be recognized (be it sound a word, a phrase etc.) are included in the training set provided to the algorithm, the training procedure should be able to adequately characterize the acoustic properties of the pattern (with no regard for or knowledge of any other pattern presented to the training procedure)This type of characterization of speech via training is called as pattern classification. Here the machine learns which acoustic properties of the speech class are reliable and repeatable across all training tokens of the pattern. The utility of this method is the pattern comparison stage with each possible pattern learned in the training phase and classifying the unknown speech according to the accuracy of the match of the patterns.

C. The Artificial Intelligence Approach

The artificial intelligence approach to speech is a hybrid of acoustic phonetic approach and the pattern recognition approach in which it exploits ideas and concepts of both methods. The artificial intelligence approach attempts to mechanize the recognition procedure according to the way a person applies intelligence in visualizing, analyzing and finally making a decision on the measured acoustic features. In particular, among the techniques used within the class of methods are the use of an expert system for segmentation and labeling. The use of neural networks could represent a separate structural approach to speech recognition or could be regarded as an implementation architecture that may be incorporated in any of the above classical approaches.

3. TECHNOLOGY COMPONENTS OF AUTOMATIC VOICE RECOGNITION

The task of automatic speaker identification for voice recognition consists of labeling an unknown voice as one of a set of known voices. The task can be carried out using several approaches, either with text dependent recognition or with text independent recognition. The choice of the recognition situation

Determines the architecture to be used. In the case of text dependent situations a time alignment the dynamic time warping (DTW) of the utterance with the test can be enough. IN the case of text independent situations a probabilistic approach might be more adequate most

computer systems for Voice recognition include the following components.

4. NEURAL NETWORKS FOR VOICE RECOGNITION

Multi-Layered Perceptron (MLP)

Multi-layered networks are capable of performing just about any linear or nonlinear computation, and can approximate any reasonable function arbitrarily well. Such networks overcome the problems associated with the perceptron and linear networks. However, while the network being trained may be theoretically capable of performing correctly, back propagation and its variations may not always find a solution. There are many types of neural networks for various applications multilayered perceptron (MLPs) are feed forward networks and universal approximations. They are the simplest and therefore most commonly used neural network architectures. In this project, MLPs have been adapted for voice recognition. A general neural structure used in this work is shown in Figure.

An MLP consists of three layers:

• An input layer

• An output layer

• An intermediate or hidden layer

Processing elements or neurons in the input layer only act as buffers for distributing the input signal xi to neurons in the hidden layer. Each neuron j in the hidden layer sums up its input signals xi after weighting them with the strengths of the respective connections wji from the input layer and computes its output yj as a function f of the sum, viz.,

$Yj=f(\Sigma W_{ji}x,)$ (1)

Training a network consists of adjusting its weights using a training algorithm. The training algorithms adopted in this study optimize the weights by attempting to minimize the sum of squared differences between the desired and actual values of the output neurons, namely:

$E= ½ \Sigma (Ydj-Yj)^2$(2)

Where dj is the desired value of output neuron j and yjis the actual output of that neuron. Each weight W_{ji} is adjusted by adding an increment $.W_{ji}$toit. W_{ji} is selected to reduce E as rapidly as possible. The adjustment is carried out over several training iterations until a satisfactorily small value of E is obtained or a given number of epoch is reached. How W_{ji}i is computed depends on the training algorithm adopted.

Training process is ended when the maximum number of epochs is reached, the performance has been minimized to the goal, the performance gradient falls below minimum gradient or validation performance has increased more than maximum fail times since the last time it decreased using validation. The learning algorithm used in this work is summarized briefly.

MLP identifiers used in this work are trained with the Levenberg-Marquardt (LM) learning algorithms. The LM is a least-square estimation method based on the maximum neighborhood idea. The LM combines the best features of the Gauss-Newton technique and the steepest-descent method, but avoids many of their limitations. In particular, it generally does not suffer from the problem of slow convergence.

Back propagation

a) Training Set

A collection of input-output patterns that are used to train the network.

b) Learning Rate

A scalar parameter, analogous to step size in numerical integration, is used to set the rate of adjustments.

c) Network Error

Total-Sum-Squared-Error (TSSE)

TSSE= 1/2 Σ Σ − (desired actual) 2(3)

Patterns outputs

Root-Mean-Squared-Error (RMSE)

RMSE=√(2*TSSE/#patterns*#outputs)(4)

From a Pattern

• Apply the value of each input parameter to each inputnode

• Input nodes computer only the identity functionCalculate Outputs for each Neuron based on the Pattern

• The output from neuron j for pattern p is Opj where kranges over the input indices and Wjk is the weight on theconnection from input k to neuron j

$$O_{pj(}\ net_{\ j)=1/(1+}\ e^{-\lambda\ net_{\ j})} \qquad (5)$$

Calculate the Error Signal for each Output Neuron

• The output neuron error signal dpj is given by

$$d_{pj}=(Tpj-pj)\ Opj\ (1-Opj)$$

T is the target value of output neuron j for pattern p Opj

is the actual output value of output neuron j for pattern p

$$net\ j=bias\ *W_{bias}+\Sigma O_{pk}W_{kj} \quad (6)$$

Calculate the Error Signal for Each Hidden Neuron

• The hidden neuron error signal dpj is given by k ranges

over the input indices and W_{kj} is the weight on the

$$\delta_{pj}= O_{pj}(1 - O_{pj})\ \Sigma\ \delta_{pk}W_{kj} \quad (7)$$

Connection from input k to neuron j neuron k and W_{kj} is theweight of the connection from hidden neuron j to the postsynapticneuron k.

Compute Weight AdjustmentsDW_{ji}at time t by

$$DW_{ji}\ (t) = ç\ d_{pj}O_{pj} \ldots..(8)$$

Apply Weight Adjustments According

$$W_{ji}\ (t+1) = W_{ji}i(t) + DW_{ji}\ (t)$$

Some Add a Momentum Term

$$A^*\ DW_{ji}\ (T-1)$$

5. VOICE CAPTURING AND PROCESSING

The first step for achieving voice recognition is to capture the sound signal of the voice. We use a standard microphone for capturing the voice signal. After this, we use the sound recorder of the Windows operating system to record the sounds that belong to the database for the voices of different persons. A fixed time of recording is established to have homogeneity in the signals. We show in Figure 4 the sound signal recorder used in the experiments.

Fig. 1. Sound recorder used in the experiments.

After capturing the sound signals, these voice signals are digitized at a frequency of 8 Khz, and as consequence we obtain a signal with 8008 sample points. This information is the one used for analyzing the voice.

6 .CONCLUSION

We have described in this paper an intelligent approach for pattern recognition for the case of speaker identification. We first described the use of monolithic neural networks for voice recognition. The objective of this paper is to provide some explanation of the speech and speaker recognition data input of the user. An algorithm which efficiently determines the optimum coordination has been successfully designed. Authentication of the user can be determined by the threshold value being set by the standard variance. One advantage of this algorithm over conventional algorithm is that false acceptance and false rejection can also be controlled by threshold value.

7. FUTURE SCOPE

A range of future improvements is possible:

• Speech independent speaker identification

• No of users can be increased

• Identification of a male female child and adult

REFERENCES

[1] O. Castillo, O. and P. Melin, "A New Approach for Plant Monitoring using Type-2 Fuzzy Logic and Fractal Theory", International Journal of General Systems, Taylor and Francis, Vol. 33, 2004, pp. 305-319.

[2] S. Furui, "Cepstral analysis technique for automatic speaker verification", IEEE Transactions on Acoustics, Speech and Signal Processing, 29(2), 1981, pp. 254-272.

[3] S. Furui, "Research on individuality features in speech waves and automatic speaker recognition techniques", Speech Communication, 5(2), 1986, pp. 183-197.

[4] J. Mariani, "Recent Advances in Speech Processing," Proc. IEEE Intl Conf. Acoustics, Speech, and Signal Processing, Glasgow, Scotland. May 1989, pp. 429-440.

[5] M.-W. Fung et al., “Improved Speaker Adaptation Using Text-Dependent Spectral Mappings,” Proc. IEEE Int’l Conf.Acoustics, Speech. and Signal Processing, New York City, 1988, pp. 131-134.

[6] D.B. Paul, “The Lincoln Robust Continuous Speech Recognizer,” Proc. IEEE Int’lConf. Acoustics, Speech, and SignalProcessing, Glasgow, Scotland, 1989, pp. 449- 452.

[7] J. Mendel, "Uncertain Rule-Based Fuzzy Logic Systems: Introduction and N Directions", Prentice-Hall, New Jersey, USA, 2001 .

[8] P. Melin, A. Mancilla, C. Gonzalez, and D. Bravo, "Modular Neural Networks with Fuzzy Sugeno Integral Response for Face and Fingerprint Recognition", Proceedings of IC-AI'04, Las Vegas, USA, 2004, pp. 91-97.

[9] S. Furui, "Speaker-dependent-feature extraction, recognition and processing Techniques", Speech Communication, 10(5-6), 1991, pp. 505-520.

[10]N.NKarnik, and J.M. Mendel, “An Introduction to Type-2 FuzzyLogic Systems”, Technical Report, University of Southern California, 1998.

[11] T. Matsui, and S. Furui, "Concatenated phoneme models for text-variable Speaker recognition", Proceedings of ICASSP'93, 1993, pp. 391-394.

[12] P. Melin, M. L. Acosta, and C. Felix, "Pattern Recognition Using Fuzzy Logic and Neural Networks", Proceedings of IC-AI'03, Las Vegas, USA, 2003, pp. 221-227

Identification of Plants Based on Leaf Images- A Review

Vandta Tiwari[1],Deepak Choudhary[2]

[1]M.Tech Scholar, [2]Associate Professor,

Department of Computer Science, Institute of Engineering & Technology, Alwar, Rajasthan

ABSTRACT Plants play an important role in our environment. Without plants there will be no existence of the earth's ecology. But in recent days, many types of plants are at the risk of extinction. To protect plants and catalogue various types of flora diversities, a plant database is an important step towards conservation of earth's biosphere. There are a huge number of plant species worldwide. To handle such volumes of information, development of a quick and efficient classification method has become an area of active research. In addition to the conservation aspect, recognition of plants is also necessary to utilize their medicinal properties and using them as sources of alternative energy sources like bio-fuel. There are several ways to recognize a plant, like flower, root, leaf, fruit etc. In recent times computer vision methodologies and pattern recognition techniques have been applied towards automated procedures of plant recognition. In this paper we review leaf architecture and various techniques for automated plant classification and recognition.

Keywords: ACH, CCD, Computer Vision, Plant Recognition, Image Processing.

1. INTRODUCTION

Leaf Analysis is a matter of interest for scientists. Classification and nomenclature of leaf is used only if leaves can be recognized. Botanists recognize leaves based on their knowledge and expertise, but for laymen leaf recognition is still a complicated task. Leaf recognition can be made simpler by using computer aided automation. A leaf recognition system should be based on a leaf classification system because there are more than one-half million of plants inhabiting the Earth and recognition without classification is a complex task [1].

Active research is needed in the area of leaf recognition to utilize huge number of plant species for their medicinal properties and also as an alternative energy sources. In recent times, computer vision methodologies and pattern recognition techniques have been applied towards automated procedures of plant recognition. Using MATLAB software the leaf recognition program becomes simple and efficient. This paper focuses on the following sections: Section II focuses on the previous work; Section III describes the Methodologies used for plant classification and recognition. Section IV includes Algorithms used for plant species classification, Section V includes Conclusion.

2. PREVIOUS WORK

Many methodologies have been proposed to analyze plant leaves in an automated fashion. A large percentage of such works utilize shape recognition techniques to model and represent the contour shapes of leaves, however additionally, color and texture of leaves have also been taken into consideration to improve recognition accuracies.Wu et al. [2], extracted 12 commonly used digital morphological features which were orthogonalized into 5 principal variables using PCA. They used 1800 leafs to classify 32 kinds of plants using a probabilistic neural network system. Wang et al. [3], employed Centroid Contour Distance (CCD) curve, eccentricity and Angle Code Histogram (ACH). Fu et al. [4] also used centroid-contour distance curve to represent leaf shapes in which an integrated approach for an ontology-based leaf classification system is proposed. For the leaf contour classification, a scaled Recognition of plants by Leaf Image using Moment Invariant and Texture Analysis CCD code system is proposed to categorize the basic shape and margin type of a leaf by using the similar taxonomy principle adopted bythe botanists. Then a trained neural network is employed to recognize the detailed tooth patterns.

3. METHODOLGY

Plant species identification requires recognizing the plant by various characteristics, such as size, form, leaf shape, flower color, odor, etc., and linking it with a common or so-called scientific name. Correct identification provides basic information about size, shape and texture of a plant and can be helpful in protecting it from various types of pests and diseases [5]. Plant species classification can be done through various ways like flower, root, leaf, fruit etc. Botanists adopted traditional classification method such as morphologic anatomy, cell biology and molecular biological approaches for doing plant species classification and recognition which is time consuming, troublesome and less efficient. However advancement in computer

technologies improves the process of plant species identification by designing automatic recognition system of plants. Plants classification can be done according to the structures of their leaf, bark, flower shapes, colors, textures and seedling morph. But if the plant classification is based on only two dimensional images then shapes of flowers, seedling and morph of plants are unsuitable because of their complex three dimensional structures [7]. Since the plant leaves are two dimensional in nature they are well suited for classification of various plant species. Leaf image can be easily transferred to computer that can automatically extract features using various image processing techniques.

- **Computer Vision**

Computer vision is concerned with the theory behind artificial systems that extract information from images [6]. The image data can take many forms, such as video sequences, views from multiple cameras, or multidimensional data from a medical scanner. Computer vision, also known as machine vision, consists of three parts: measurement of features, classes of leaves based on the extracted features. Furthermore, the system uses the results of the classification scheme in identifying the class of new leaf images.

- **Image Pre-processing**

Before the operations, some of the leaf images are rotated manually for helping the program to arrange leaf apex direction to the right side. Afterwards, automatic pre-processing techniques are applied to all of the leaf images. These pre-processing steps are illustrated on an image as seen in Figure 1, while ignoring the color information.

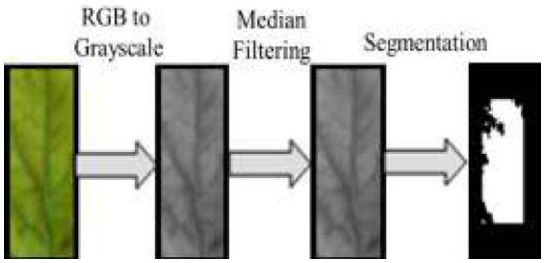


Figure 1: Pre-processing Steps of Image

As a result, only Gray component for each pixel is computed from the color image by:

$Gray = 0.299 * R + 0.578 * G + 0.114 * B$

Where, R, G and B correspond to the color of the pixel [8, 9], respectively. The rectangle of interest (ROI) of the leaf image should include all the pixels their Gray values are smaller than a specific threshold [10], and then the binary image of the leaf is retrieved. In this approach the threshold is automatically gotten according to the histogram of the leaf Gray image. Then the contour of leaf can be extracted.

- **Measurement/Extraction of Features**

Image processing technologies are used to extract a set of features/measurement that characterize or represent the image [7]. The values of these features provide a concise representation about the information in the image. For example, a set of features that characterize a triangle could be the length if each side of the triangle.

- **Pattern classification**

Pattern classification [6] is the organization of patterns into groups of pattern sharing the same set of properties. Given a set of measurement of an unknown object and the knowledge unknown object belongs could be made. For example, if a set of features/measurements is extracted from a leaf, a decision about the possible class of the leaf can be made. Pattern classification may be statistical or syntactic.

- **Pattern Recognition**

Pattern recognition [6] is the process of classifying data or patterns based on the knowledge/information extracted from patterns. The patterns to be classified usually groups of measurements or observations defining points in an appropriate multidimensional space.

- **Histogram**

A histogram is a way to graphically represent the distribution of data in a dataset. Each data point is placed into a bin based on its value. The histogram is a plot of the number of data points in each bin. In scientific experiments, histograms are useful in characterizing the spread of data from repeated trials and for determining the probability of given measurements [11].

- **Histogram stretching is used to enhance the contrast**

Contrast is the difference between maximum and minimum pixel intensity. An important class of point operations is based upon the manipulation of an image histogram or a region histogram. The most important examples are described below. Frequently, an image is scanned in such a way that the resulting brightness values do not make full use of the available dynamic range. By stretching the histogram over the available dynamic range we attempt to correct this situation. If the image is intended to go from brightness 0 to brightness 2B-1, then one generally maps the 0% value (or minimum as defined) to the value 0 and the 100% value (or maximum) to the value 2B-1 [11]. The appropriate transformation is given by:

$$b[m,n] = (2^B - 1) * \frac{a[m,n] - minimum}{maximum - minimum}$$

This formula, however, can be somewhat sensitive to outliers and a less sensitive and more general version is given by:

$$b[m,n] = \{0 \quad a[m,n] \leq p_{low}\,\%\,(2^B - 1) * \frac{a[m,n] - p_{low}\,\%}{p_{high}\,\% - p_{low}\,\%} ghummtheleafimages.p_{low}\,\% < a[m,n] < p_{high}\,\% \quad (2^B - 1) \quad a[m,n] \geq p_{high}\,\%$$

We can increase the contrast of the image. The formula for stretching the histogram of the image to increase the contrast is:

$$g(x,y) = \frac{f(x,y) - f_{min}}{f_{max} - f_{min}} * 2^{bpp}$$

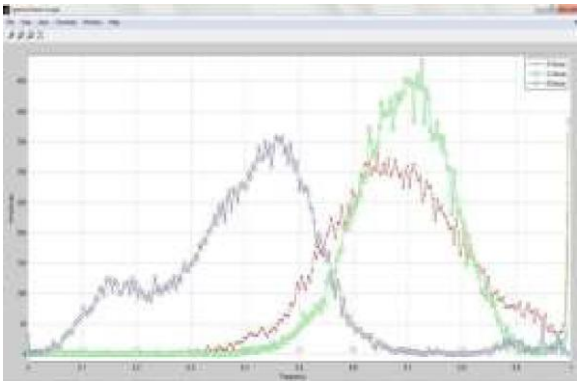


Figure 2: Histogram of Leaf for optical image

4. ALGORITHMS USED FOR PLANT SPECIES CLASSIFICATION

The classification algorithm implemented for accurate identification of the plants based on Leaf images.

- **K-means clustering**

K-means clustering is an algorithm to classify the objects based on attributes/features into number of groups where Kis a positive integer. K-means clustering is a supervised learning algorithm and utilized a prior knowledge of the number of clusters.

- **The k-nearest neighbor algorithm**

The k-nearest neighbor algorithm is the simplest of all machine learning algorithms: an object classification depends on the majority vote of its neighbors, with the object being assigned to the class most common amongst its k nearest neighbors. Guetal. [12] Used the k-nearest neighbor algorithm for doing plant species classification.

- **Move median centers (MMC) hyper sphere**

Du et al. [13] used move median centers (MMC) hypersphere classifier to classify plants based on shape-related features of leaf such as aspect ratio, rectangularity, area ratio of convex hull, perimeter ratio of convex hull, sphericity, circularity, eccentricity, form factor, and invariant moments.

- **Probabilistic neural network**

Wu et al.[14] used a probabilistic neural network for classification of leaf images on the basis of 12 leaf features.

- **SVM (Support Vector Machines)**

SVM (Support Vector Machines) is based on the concept of decision planes that define decision boundaries. Hongfei [10] utilized SVM for identification of Camellia species.

5. CONCLUSION

Plants play an important role in human life and provide required information for the development of human society.There are various algorithms used for classification as per literature survey. Most of these researches have been done on standard 32 species of plants. However these species have been tested on at the most 2 techniques of classification algorithms. Botanists recognize leaves based on their knowledge and expertise, but for laymen leaf recognition is still a complicated task. A leaf recognition system should be based on a leaf classification system because there are more than one-half million of plants inhabiting the earth and recognition without classification is a complex task.In leaves recognition research, a lot has been done about general features extraction or recognition between different classes of objects. In case of specific domain recognition, taking into account the unique characteristics that belong to this category, improves the performance of the system

REFERENCES

[1] SimranjitKaurDhindsa, Rajbir Singh, "Plant Identification and Classification Using Fuzzy Methods of Segmentation", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 9, September 2014 ISSN: 2277 128X.

[2] S. Wu, F. Bao, E. Xu, Y. Wang, Y. Chang, and Q. Xiang. A leaf recognition algorithm for plant classification using probabilistic neural network. In 7th IEEE International Symposium on Signal Processing and Information Technology, Cairo, Egypt, 2007

.

[3]]Z. Wang, Z. Chi, and D. Feng. Shape based leaf image retrieval. IEEE P-VisImage Sign. 150:34–43, 2003.

[4] H. Fu, Z. Chi, D. Feng, and J. Song. Machine learning techniques for ontology-based leaf classification. In 8th IEEE International Conference on Control, Automation, Robotics and Vision, Kunming, China, 2004

.

[5] Gurpreetkaur, Himanshumonga (2012) "Classification of Biological Species Based on Leaf Architecture" IRACST- International Journal Of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 2, No.2.

[6] D.Warren (1997) "Automated leaf shape description for variety testing in chrysanthemums" in proc. 6th Int. Conf. Image Process and its Applicant. , Duplin, Ireland.

[7] YotismitaChaki, Ranjan Parekh (2011)" Plant Leaf Recognition using shape based Features and Network classifiers" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol.2.

[8] R. C. Gonzalez and R. E. Woods. Digital image processing, 2nd edition. Prentice Hall, Upper Saddle River, NJ, 2004.

[9] M. Sonka, V. Hlavac, and R. Boyle. Image processing, analysis, and machine vision, 2nd edition. Cengage Learning, Stamfort, CT, 2003. Otsu, N. A threshold selection method from gray-level histograms. IEEE T. Syst.Man. Cyb. 9:62–66, 1979

[10] The MathWorks Inc. MATLAB 7.0 (R14SP2). The MathWorks Inc., 2005.

[11] X. Gu et al.,Wang.: Leaf recognition based on the combination of wavelet transform and Gaussian interpolation,ICIS, vol. 3644/2005, pp. 253-262, 2005.

[12] J.X. Du et al.: Leaf shape based plant species recognition, Applied Mathematics and Computation, vol.185, issue 2, Amsterdam, Elsevier, 2007, pp.883-893.

[13] S.Wu et al: A Leaf Recognition Algorithm for Plant Classification Using Probabilistic Neural Network, in Proc. Signal Process. And Inform. Technology, IEEE Int. Symp., Cairo, Egypt, 2007

Implementation of security issues in routing algorithm in mobile ad-hoc network

Ashok Kumar Meena[1], Pratap Singh Patwal[2],Rohit Singhal

[1]M.Tech Scholar, [2,3]Associate Professor,

Department of Computer Science, Institute of Engineering & Technology, Alwar, Rajasthan

ABSTRECT

Implementation of Mobile ad hoc network in retail business at a lower cost. While the retail industry begins to embrace this new technology and install in mobile ad-hoc wireless network. The issues of security become highly challenging to both public and private organizations. This paper will discuss the issues with a systematic approach to address the security of mobile ad hoc network infrastructure. We present some cost efficient but effective solutions to improve the security based on the industrial standards and cutting edge technology. From these algorithm can able to find out the malicious attackers correctly from the source to destination. Also analyze the performance of the entire network using simulation parameters such as packet delivery ratio and routing overhead. The fifth generation of Wi-Fi and new standards of telecommunication protocols enable the implementation of Mobile ad hoc network in retail business at a lower cost. While the retail industry begins to embrace this new technology and install a Wi-Fi hotspot in their stores and shopping carts, the issues of security become highly challenging to both public and private organizations. This paper will discuss the issues with a systematic approach to address the security of mobile ad hoc network infrastructure. We present some cost efficient but effective solutions to improve the security based on the industrial standards and cutting edge technology.

Keywords: security, ad hoc network, mobile commerce

1. INTRODUCTION

1.1 Wireless network

Wireless communication between mobile users is becoming more popular. This due to recent technological advances in laptop computers and wire

Substantial progress has been achieved in solving the routing challenge in mobile wireless ad hoc networks. The Ad hoc On demand Distance Vector protocol (AODV) and the Dynamic Source Routing protocol (DSR) are among the most prominent ad hoc routing protocols. These protocols provide a basic routing functionality that is sufficient for conventional applications such as file transfer ore-mail download. However, ad hoc networks are also an interesting platform for more demanding applications such as Voice over IP (VoIP), which are very susceptible to larger delays, jitter, and packet losses. In order to support such applications, it is not sufficient to provide a basic routing functionality alone. Several proposals for routing schemes exist that are sup-posed to find routes fulfilling certain QoS demands of applications. In these, many assumptions have been adopted from wired networks. This article discusses the fundamental differences between wired networks and wireless ad-hoc networks which are important for QoS provisioning. An ad-hoc network is a collection of wireless mobile nodes dynamically forming a temporary network. In this network topology may change rapidly due to mobility condition. Here all the nodes act as either source or destination; it will transmit and also receive the packets simultaneously. It does not have any centralized infrastructure and used to generate distributed network. In centralized, nodes will transmit the packet via center server and also dependent. But in MANET used to transmit the packets from source to destination via intermediate nodes and also independently. It will randomly create the topology based on the routing table source will transmit the packets to the destination. Figure 1 shows the [MANET] Mobile Ad hoc Network architecture. S denotes the source, D denotes the destination between the source and destination nodes are intermediate nodes act as co-operative nodes. All the mobile nodes are generated randomly in a dynamic architecture. An intermediate node does not transmit the packet in a certain time, intruders may attack the node and the packet will be lost. Wireless ad-hoc network is a decentralized type of wireless network where the devices are PDAs, cell phones, sensors, laptop etc. The Network is ad-hoc because it does not rely on a preexisting infrastructure, such as routers in wired network or access points in managed (infrastructure) wireless networks. The node can transmit data to another node if it is within its

frequency range. Each node participates in routing by forwarding data for the rnodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity

Ad-hoc networks use flooding for forwarding the data. In flooding, the source simply broadcasts the packet to its neighbor node via a MAC layer(Medium access control layer)Ad hoc network refers to a mode of operation of IEEE 802.11 wireless networks, which is a set of implementing wireless local area network(WLAN) computer communication in the 2, 4, 3.6 and 5 GHz frequency bands.

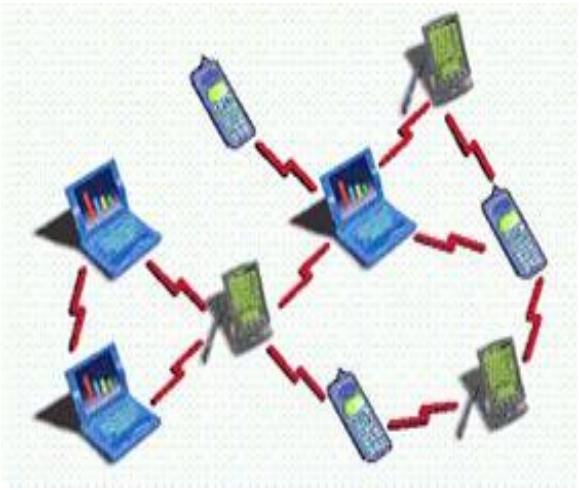


Fig.1 Mobile ad-hoc network

1.2 QUALITY OF SERVICE

Quality of service (QoS) is the performance level of a service offered by the network to the user. The goal of QoS provisioning is to achieve a more deterministic network behavior, so that information carried by the network can be better delivered and network resources can be better utilized. A network or a service provider can offer different kinds of services to the users. Here, a service can be characterized by a set of measurable prespecified service requirements such as minimum bandwidth, maximum delay, maximum delay variance (jitter), and maximum packet loss rate. After accepting a service request from the user, the network has to ensure that service requirements of the users flow are met, as per the agreement, throughout the duration of the flow (a packet stream from the source to the destination). In other words, the network has to provide a set of service guarantees while transporting a flow. After receiving a service request from the user, the first task is to find a suitable loop-free path from the source to the destination that will have the necessary resources available to meet the QoS requirements of the desired service. This process is known as QoS routing. After finding a suitable path, are source reservation protocol is employed to reserve necessary resources along that path.QoS guarantees can be provided only with appropriate resource reservation techniques.

For example, consider the network shown in where BW and D represent available bandwidth in Mbps and delay in milliseconds.

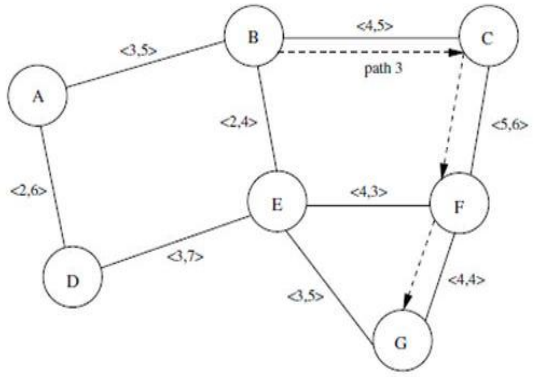


Fig2.an example of Qos routing in wireless mobile ad-hoc network

Suppose a packet-flow from node B to node G requires a bandwidth guarantee of 4 Mbps.QoS routing searches for a path that has sufficient bandwidth to meet the bandwidth requirement of the flow. Here, 6 paths are available between nodes B and G as shown in Table. QoS routing selects path 3 (i.e., B-C-F-G) because, out of the available paths, path 3 alone meets the bandwidth constraint of 4 Mbps for the flow. The end-to-end bandwidth of a path is equal to the bandwidth of the bottleneck link (i.e., link having minimum bandwidth among all the links of a path). The end-to-end delay of a path is equal to the sum of delays of all the links of a path. Clearly path 3 is not optimal in terms of hop count and/or end to-end delay parameters, while path 1 is optimal in terms of both hop count and end-to-end delay parameters. Hence, QoS routing has to select a suitable path that meets the QoS constraints specified in the service request made by the user

Table1.path form node B to node G:-

Available paths from node *B* to node *G*

No.	Path	Hop count	BW (Mbps)	Delay (ms)
1	$B \rightarrow E \rightarrow G$	2	2	9
2	$B \rightarrow E \rightarrow F \rightarrow G$	3	2	11
3	$B \rightarrow C \rightarrow F \rightarrow G$	3	4	15
4	$B \rightarrow C \rightarrow F \rightarrow E \rightarrow G$	4	3	19
5	$B \rightarrow A \rightarrow D \rightarrow E \rightarrow G$	4	2	23
6	$B \rightarrow A \rightarrow D \rightarrow E \rightarrow F \rightarrow G$	5	2	25

1.3 RELATED WORKS

In the recent period lot of research has been done in QOS based, multi-path and node disjoint routing. Lately, the upcoming concern is the energy issues in mobile ad hoc networks (MANETs) The recent studies extensively focused on the multipath discovering extension of the on-demand routing protocols in order to alleviate single-path problems like AODV and DSR, such as high route discovery latency, frequent route discovery attempts and possible improvement of data transfer throughput. The AODVM (AODV Multipath) AOMDV, is a multipath extension to AODV. These provide link-disjoint and loop free paths in AODV.

Cross-layered multipath AODV (CM-AODV) , selects multiple routes on demand based on the signal-to-interference plus noise ratio (SINR) measured at the physical layer. The Multipath Source Routing (MSR) protocol is a multipath extension to DSR uses weighted round robin packet distribution to improve the delay and throughput. (Split Multipath Routing) is another DSR extensions, which selects hop count limited and maximally disjoint multiple routes. Node-Disjoint Multipath Routing (NDMR), provides with node-disjoint multiple paths. Other energy aware multipath protocols which give disjoint paths are Grid-based Energy Aware Node-Disjoint Multipath Routing Algorithm GEANDMRA), Energy Aware Source Routing (EASR) and Energy Aware Node Disjoint multipath Routing(ENDMR). The Lifetime-Aware Multipath Optimized Routing (LAMOR) is based on the lifetime of a node which is related to its residual energy and current traffic conditions. Cost- effective Lifetime Prediction based Routing (CLPR), combines cost efficient and lifetime predictions based routing. Minimum Transmission Power Routing (MTPR), Power-aware Source Routing(PSR).

2. SECURITY ISSUES IN MANETs

Security is the major issue in wireless Ad Hoc Networks and actually ought to receive a complete analysis of it than being presented as a part of the study on Ad Hoc Networks. The use of wireless links renders an ad hoc network susceptible to link attacks ranging from denial of service, passive eavesdropping to active impersonation, message replay, and message distortion. Eavesdropping might give an adversary access to secret information, violating confidentiality. Active attacks might allow the adversary to delete messages, to inject erroneous messages, to modify messages, and to impersonate a node, thus violating availability, integrity, authentication, and non-repudiation. Nodes, roaming in a hostile environment (e.g., a battlefield) with relatively poor physical protection, have non-negligible probability of being compromised. Therefore, we should not only consider malicious attacks from outside a network, but also take into account the attacks launched from within the network by compromised nodes. Therefore, to achieve high survivability, ad hoc networks should have a distributed architecture with no central entities. Introducing any central entity into our security solution could lead to significant vulnerability; that is, if this centralized entity is compromised, then the entire network is subverted.

An ad hoc network is dynamic because of frequent changes in both its topology and its membership (i.e., nodes frequently join and leave the network). Trust relationship among nodes also changes, for example, when certain nodes are detected as being compromised.

2.1 UNRELIABLE WIRELESS CHANNEL— the wireless channel is prone to bit errors due to interference from other transmissions, thermal noise, shadowing, and multipath fading effects. This makes it impossible to provide hard packet delivery ratio or link longevity guarantees.

2.2 NODE MOBILITY— the nodes in a MANET may move completely independently and randomly as far as the communications protocols are concerned. This means that topology information has a limited lifetime and must be updated frequently to allow data packets to be routed to their destinations. Again, this invalidates any hard packet delivery ratio orlink stability guarantees. Furthermore, a QoS state which islink- or node position dependent must be updated with a frequency that increases with node mobility.

2.3 LIMITED DEVICE RESOURCES— to some extent this is an historical limitation, since mobile devices are

becoming increasingly powerful and capable. However, it still holds true that suchdevices generally have less computational power, less memory,and a limited (battery) power supply, compared to devicessuch as desktop computers typically employed in wired networks. This factor has a major impact on the provision of QoSassurances, since low memory capacity limits the amount ofQoS state that can be stored, necessitating more frequentupdates, which incur greater overhead. Additionally, QoSrouting generally incurs a greater overhead than best-effortrouting in the first place, due to the extra information beingdisseminated. These factors lead to a higher drain on mobilenodes' limited battery power supply.

3. ROUTING PROTOCOLS

3.1 Why Routing Protocols are the main issue In Ad Hoc networks

Routing support for mobile hosts is presently being formulated as mobile IP technology when the mobile agent moves from its home network to a foreign (visited) network, the mobile agent tells a home agent on the home network to which foreign agent their packets should be forwarded. In addition, the mobile agent registers itself with that foreign agent on the foreign network. Thus, the home agent forwards all packets intended for the mobile agent to the foreign agent, which sends them to the mobile agent on the foreign network. When the mobile agent returns to its original network, it informs both agents (home and foreign) that the original configuration has been restored. No one on the outside networks need to know that the mobile agent moved.

But in Ad Hoc networks there is no concept of home agent as it itself may be moving.

Supporting Mobile IP form of host mobility requires address management, protocol inter-operability enhancements and the like, but core network functions such as hop by hop routing still presently rely upon preexisting routing protocols operating within the fixed network. In contrast, the goal of mobile ad hoc networking is to extend mobility into the realm of autonomous, mobile, wireless domains, where a set of nodes, which may be combined routers and hosts, themselves form the network routing infrastructure in an ad hoc fashion. Hence, the need to study special routing algorithms to support this dynamic topology environment. Routing protocols for mobile ad-hoc networks have to face the challenge of frequently changing topology, low transmission power and asymmetric links.

3.2 Ad Hoc Routing Protocols:

A number of routing protocols have been suggested for ad-hoc networks. These protocols can be classified into two main categories:

Table driven routing protocols

Source initiated on demand routing protocols

Table Driven Routing Protocols:

Table-driven routing protocols attempt to maintain consistent, up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information, and they respond to changes in network topology by propagating updates throughout the network in order to maintain a consistent network view. The areas in which they differ are the number of necessary routing-related tables and the methods by which changes in network structure are broadcast.

Source Initiated On Demand Routing:

A different approach from table-driven routing is source-initiated on demand routing. This type of routing creates routes only when desired by the source node. When a node requires a route to a destination, it initiates a route discovery process within the network. This process is completed once a route is found or all possible route permutations have been examined. Once a route has been established, it is maintained by a route maintenance procedure until either the destination becomes inaccessible along every path from the source or until the route is no longer desired.

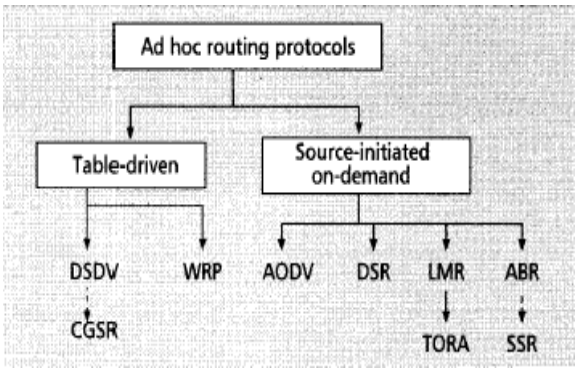


Fig. 3.Categorization of ad hoc routing protocols.

TABLE DRIVEN ROUTING PROTOCOLS

Destination Sequenced Distance Vector Routing Algorithm:

The Destination Sequenced Distance Vector (DSDV) Routing Algorithm is based on the idea of the Distributed Bellman Ford (DBF) Routing Algorithm with certain improvements. The primary concern with using a Distributed Bellman Ford algorithm in Ad Hoc environment is its susceptibility towards forming routing loops and counting to infinity problem. DSDV guarantees loop free paths at all instants.

Each node maintains a routing table, which contains entries for all the nodes in the network. Each entry consists of:

- the destination's address
- the number of hops required reaching the destination (hop count)

Whenever a node B comes up, it broadcasts a beacon message ("I am alive message") stamping it with a locally maintained sequence number. The nodes in its neighborhood listen to this message and update the information for this node. If the nodes do not have any previous entry for this node B, they simply enter B's address in their routing table, together with hop count and the sequence number as broadcasted by B. If the nodes had previous entry for B, then sequence number of broadcasted information is compared to the sequence number stored in the node for estimation B. If the message received has a higher sequence number, then this means that the node B has propagated a new information about its location so the entry must be updated in accordance with the new informationreceived. The information with a newer sequence number is definitely new as the node B itself stamps sequence number.

4. Conclusion

Ad Hoc Networks is an area that is being widely researched these days and is a very fast growing area. Much work still is left to be done in this field for it to be commercially viable. It is the technology that is providing the stepping blocks to the evolution of 4G. Power Control is a major area of improvement and also they need to be made more secure. Ad Hoc Networks have started to be implemented in the field today in battlefields and also in disaster struck areas. As time goes by we can see more applications of Ad Hoc Networks.

Starting from the observation that guaranteeing the validity of cached paths at a node is critical to achieving good performance in reactive routing protocols, in this paper, we proposed a new cache mechanism, based on the notion of caching zone, which proactively removes stale information from the caches of all the nodes in a MANET.

REFERENCES

[1] Abramov, R., & A. Herzberg (2013). TCP Ack storm DoS attacks. Computers & Security, 33, 12-27.

[2] Adnane, A., Bidan, C., & de Sousa Júnior, R. T. (2013).Trust-based security for the OLSR routing proto- col. Computer Communications, 36(10), 1159-1171

[3]. Agah, A., Basu, K., & Das, S. K. (2006). Security enforcement in wireless sensor networks: A framework based on non-cooperative games. Pervasive and Mobile Computing, 2(2), 137-158.

[4] Almomani, I., Al-Banna, E., & Al-Akhras, M. (2013).Logic-Based Security Architecture for Systems Providing Multihop Communication.International Journal of Distributed Sensor Networks, 2013, 1- 17

[5] .Bankovic, Z., Fraga, D., Manuel Moya, J., Carlos Vallejo, J., Malagón, P., Araujo, Á., ...& Nieto-Taladriz, O. (2011).

[6] Improving security in WMNs with reputation systems and self-organizing maps. Journal of Network and Computer Applications, 34(2), 455-463.

[7] Boukerche, A., &Ren, Y. (2008).A trust-based security system for ubiquitous and pervasive computing environments. Computer Communications, 31(18), 4343-4351.

[8] Burmester, M., Le, T. V., &Yasinsac, A. (2007). Adaptive gossip protocols: Managing security and redun- dancy in dense ad hoc networks. Ad Hoc Networks, 5(3), 313-323.

[9] Chen, P.-T.& Cheng, J. Z. (2010).Unlocking the promise of mobile value-added services by applying new collaborative business models. Technological Forecasting and Social Change, 77(4), 678-693.

[10] Cionca, V., Newe, T., &Dădârlat, V. T. (2012). Configuration tool for a wireless sensor network integrated security framework." Journal of Network and Systems Management 20(3), 417-452.

[11] Dahlberg, T., Mallat, N., Ondrus, J., &Zmijewska, A. (2008). Past, present and future of mobile payments research: A literature review. Electronic Commerce Research and Applications, 7(2), 165-181.

[12] Datta, R., &Marchang, N. (2012). Chapter 7 - Security for mobile ad hoc networks. In S. K. Das, K. Kant, & Zhang, Handbook on securing cyber-physical critical infrastructure (pp.147-190). eDigitalResearch (2013). Survey

Mobile Ad Hoc Network Comparison b/w Proactive & Reactive Routing Protocols

Pavan Kumar[1], Vedant Rastogi[2],Dinesh Sharma[3]
[1]M.Tech Scholar, [2]Associate Professor, [3]Assistant Professor
Department of Computer Science, Institute of Engineering & Technology, Alwar, Rajasthan

ABSTRACT

An Ad hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any centralized administration or infrastructure. Such networks have no fixed topology due to the high degree of node mobility. Hence, efficient and reliable routing is one of the key challenges in mobile ad hoc networks. Many routing algorithms have been proposed and developed for accomplishing this task. Therefore, it is difficult to determine which protocol performs best under a number of different scenarios. Hence, this paper presents review and a comparison of the typical representatives of routing protocols designed for MANETs.

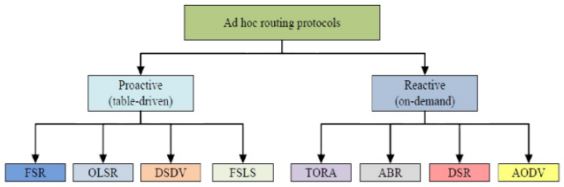
A routing protocol is used to facilitate communication in ad hoc network. The primary goal of such a routing protocol is to provide an efficient and reliable path between a pair of nodes. The routing protocols for ad hoc network can be categorized into three categories: table driven, on demand and hybrid routing. The table driven and hybrid routing strategies require periodic exchange of hello messages between nodes of the ad hoc network and thus have high processing and bandwidth requirements. On the other hand on demand routing strategy creates routes when required and hence is very much suitable for ad hoc network.

KEYWORDS:
Mobile Ad Hoc Networks, Routing protocols, DSDV, DSR, AODV, review

1. INTRODUCTION

With the continuous development of network technology, the wireless network gets more and more attention as its convenience and scalability. A mobile ad hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless [1]. The growth of laptops and Wi-Fi wireless networking have made MANETs a popular research topic. Routing protocols are classified as proactive (example DSDV, OLSR) and reactive (example DSR, AODV) on the basis of their routing methods[8]. Proactive protocols determine routes independent of traffic pattern. Traditional link-state and distance-vector routing protocols are proactive. Reactive protocols maintain routers only if needed. Routing [1] is the process in which a route from a source to a destination node is identified. In order to facilitate communication within MANET, a routing protocol is used to discover routes between nodes. The primary goal of such a routing protocol is to ensure correct and efficient route establishment between a pair of nodes so that messages are delivered in a timely manner. The routing protocols for mobile ad hoc network can be categorized on the basis of how routing information is acquired and maintained by mobile nodes [17] into three categories as follows:

Proactive routing or Table driven routing
Reactive routing or on demand routing
Hybrid routing



Wireless communication is an emerging and upcoming technology that will allow users to access information and services electronically, irrespective of their geographic location. There are solutions to these demands, one being wireless local area network (based on IEEE 802.11standard). However, there is increasing demand for connectivity in situations/places where there is no base station / infrastructure available. This is where ad hoc network came into existence. Wireless networks can be classified into infrastructure networks and infrastructure less networks or mobile ad hoc networks (MANETs).There are currently two variations of mobile wireless networks infrastructure and Infrastructure less networks. The infrastructure networks, also known as Cellular network,

have fixed and wired gateways. They have fixed base stations that are connected to other base stations through wires. The transmission range of a base station constitutes a cell. All the mobile nodes lying within this cell connects to and communicates with the nearest bridge (base station). A hand off occurs as mobile host travels out of range of one Base Station and into the range of another and thus, mobile host is able to continue communication seamlessly throughout the network.Example of this type includes office wireless local area networks (WLANs)[18].

2. RELATED WORK

A number of routing protocols have been proposed and implemented for MANETs in order toenhance the bandwidth utilization, minimum energy consumption, higher throughputs, lessoverheads per packet, and others. Different routing protocols have used different metrics todetermine an optimal path between the sender and the recipient. All these protocols have theirown advantages and disadvantages.

Any MANET routing protocol exhibits two types of properties:

• Qualitative such as loop freedom, security, demand based routing, distributed operation, multi-path routing etc.

• Quantitative such as throughput, delay, route discovery time, packets delivery ratio, jitter etc.

Obviously, most of the routing protocols are both qualitatively and quantitatively enabled. A lotof simulation studies were carried out in paper [3], [16] to analyze the quantitative properties of routing protocols. The emphasis in this paper is concentrated on the study, survey and comparison of most popular routing protocols DSDV, AODV & DSR, as these are best suited for ad-hoc networks. Our workis to methodically investigate the characteristics of proactive and on-demand routing approaches by studying some of the protocols. The next section describes the classification of routing protocols.

3. CLASSIFICATION OF ROUTING PROTOCOLS

The inadequate and limited resources in MANETs have made designing of an efficient and reliable routing strategy a very challenging task. An intelligent routing algorithm is required to efficiently use these limited resources while at the same time being adaptable to the changing network conditions such as network size, traffic density, nodes mobility, network topology and broken routes. Numerous routing protocols have been proposed and developed for ad hoc networks. Such protocols must deal with the limited resources available with these networks, which include high-power consumption, low bandwidth and high mobility.

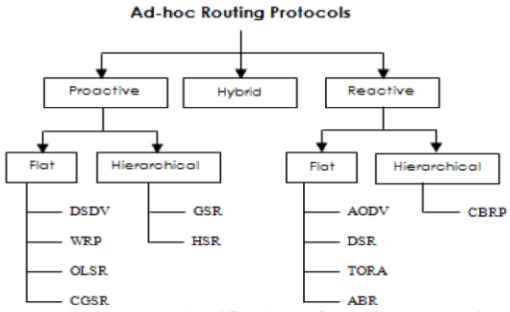


Figure 1. Classification of Routing Protocols

3.1 Table-driven Routing Protocols (Proactive)

Proactive protocols are also known as “table-driven” routing protocols. In this protocol, each andevery node maintains complete information about the network topology by continuously evaluating routes to all the nodes. Hence, they maintain consistent and up-to-date routing information. These protocols are known as proactive since they maintain the routing information before it is needed. There are various existing proactive routing protocols. The areas in which they differ are broadcast. Some of the existing proactive protocols are Destination-Sequenced Distance Vector (DSDV) [5], Global State Routing (GSR)[13].

3.2 On-demand Routing Protocols (Reactive)

A different approach from table-driven routing is on-demand routing. In this approach, a routing path is discovered only when the need arises. These are called reactive since it is not necessary to maintain routing information at the nodes if there is no communication. When needed, a route discovery operation in turn invokes a route-determination procedure. The discovery procedure terminates either when a route has been found or no route available after examination of all the route permutations. Some of the existing reactive protocols are Ad hoc On-Demand Distance Vector (AODV) [6], Dynamic Source Routing (DSR) [2].

	Table-driven	On-demand
Availability of Routing Information	Always available (in routing table)	Available when needed
Route Updates	Periodic	When requested
Routing Structure	Both flat and hierarchical	Mostly flat
Storage Requirements	High	Usually lower than proactive
Routing Overhead	Proportional to the size of network	Proportional to the number of communicating nodes
Latency	Small	Most applications suffer a long delay

4. ROUTING PROTOCOLS

This section describes some of the important proactive and reactive routing protocols.

4.1 Destination-Sequence Distance Vector (DSDV) routing protocol

The DSDV protocol described in [6] is a table-driven protocol based on the classical Bellman-
Ford algorithm [9].

Advantages

Guarantees loop free paths.

Sequence number ensures the freshness of routing information available in the routingtable.

DSDV avoids extra traffic by using incremental updates instead of full dump updates.

DSDV maintains only the best path or shortest path to every destination. Hence, amount ofspace in routing table is reduced.

Limitations

Large amount of overhead due to the requirement of periodic update messages, whichmakes them un-effective in large networks.

It doesn't support multi path routing.

Wastage of bandwidth due to needless advertising of routing information even if there is nochange in the network topology

4.2 Dynamic Source Routing (DSR)

DSR [2], a reactive unicast protocol is based on source routing algorithm. In source routing, each data packet contains complete routing information to reach its destination. There are two major phases in DSR: route discovery and route maintenance.

Advantages

• Reduction of route discovery overheads with the use of route cache.

• Supports multi path routing.

• Does not require any periodic beaconing or hello message exchanges.

Limitations

• DSR is not very effective in large networks, as the amount of overhead carried in thepacket will continue to increase as the network diameter increases.

• Because of source routing, packet size keeps on increasing with route length.

• Being a reactive protocol, DSR suffers from high route discovery latency.

4.3 Ad-Hoc On-Demand Distance Vector (AODV) Routing protocol

As a reactive protocol, AODV [7] only needs to maintain the routing information about the activepaths. Every node keeps a next-hop routing table, which includes only those destinations to which it currently has a route. A route entry in the routing table expires if it has not been used for a pre specified expiration time. Moreover, AODV adapts the destination sequence number technique used by DSDV.

Advantages

AODV can handle highly dynamic MANETs.

Less amount of storage space as compared to other reactive routing protocols, since routinginformation which is not in use expires after a pre-specified expiration time.

Supports multicasting.

Limitations

AODV lacks an efficient route maintenance technique. The routing information is alwaysobtained on demand [26].

Similar to DSR, AODV also suffers from high route discovery latency.

More number of control overheads due to many route reply messages for single routerequest.

5. COMPARATIVE STUDY

This section provides comparative analysis between routing protocols described in the previous section Time complexity is defined as the number of steps needed to perform a protocol operation and communication complexity is the number of messages needed to perform a protocol operation [10], [17]. Also, the values for these metrics represent the worst case behavior. Control traffic overhead and loop-free properties are two important issues with proactive routing protocols in MANETs. The proactive routing used for wired networks normally have predictable control traffic overhead because topology changes rarely and most routing updates are periodically propagated.

	DSDV	AODV	DSR
Protocol Type	Distance vector	Distance vector & Source routing	Source routing
Route Computation	Proactive	Reactive	Reactive
Routing Structure	Flat	Flat	Flat
Update Period	Periodic and as required	Event-driven	Event-driven
Loop-free	Yes	Yes	Yes
Multicast capability	No	Yes	No
Routing metric	Shortest path	Freshest & shortest path	Shortest path
Updates transmitted to	Neighbors	Source	Source
Hello message requirement	No	Yes	No
Multiple routes	No	No	Yes
Route maintained in	RT	RT	RC
Utilizes sequence numbers	Yes	Yes	No
Utilizes route cache/table expiration times	No	Yes	No
Time Complexity (initialization/post failure)	O(d)	O(2d)	O(2d)
Communication Complexity (initialization/post failure)	O(N)	O(2N)	O(2N)
Storage Complexity	O(N)	O(D')	O(d)
Advantages	Loop-free	Adaptable to highly dynamic topologies	Multiple routes
Limitations	High overhead	Scalability problems, large delays	Scalability problems due to source routing & flooding

Table 2: Comparison of DSDV, AODV and DSR

	DSDV	AODV	DSR
Delivery of ratio packet	98 bytes	512 bytes	512 bytes
End to End delay packet	6-8m/s	10m/s	10-25m/s
Transmitting rate packet	15 second	10 second	10 second
No.of node packet	40	40-100	25-50
Topology size packet	1000*1000m	1000*1000m	500*500m
Developed Protocol	Perkins-1994	Perkins-1999	Johnson-1996

Table 3: Comparison of DSDV, AODV and DSR

6. CONCLUSION

This article described the classification of several routing schemes according to the routing strategy. We discussed some important characteristics of the two routing strategies (table-drive and on-demand). In this paper, an effort has been made to concentrate on the comparative study of DSDV, AODV& DSR. Moreover, a single routing protocol can't perform best in all situations. So, the choice of routing protocol should be done carefully according to the requirements of the specific application. The focus of the study in our future research work is to propose an extension of the existing conventional routing protocols which will be better in terms of security, throughput, efficient utilization of limited resources and quality of service.DSR and AODV both use on-demand route discovery, but with different routing mechanics. In particular, DSR uses source routing and route caches, and does not depend on any periodic or timer-based activities. DSR exploits caching aggressively andmaintains multiple routes per destination. AODV, on the other hand, uses routing tables, one route per destination, and destination sequence numbers, a mechanism to prevent loops and to determine freshness of routes. The general observation from the simulations that for application-oriented metrics such as packet delivery fraction and delay AODV,out performs DSR in more "stressful" situations (i.e., smaller number of nodes and lower load and/or mobility), with widening performance gaps with increasing stress (e.g., more load, higher mobility).

References

[1] MehranAbolhasan, TadeuszWysocki, and ErykDutkiewicz. "A review of routing protocols formobile ad hoc networks". Technical report, Telecommunication and Information Research Institute,University of Wollongong, Wollongong, NSW 2522; Motorola Australia Research Centre, 12 LordSt., Botany, NSW 2525, Australia, 2003.

[2] David B. Johnson and David A. Maltz."Dynamic source routing in ad hoc wireless networks".Technical report, Carnegie Mellon University, 1996.

[3] J. Broch, David B. Johnson, David A. Maltz, "A performance comparison of multi-hop wireless adhoc network routing protocols". Proc. MOBICOM, 1998, 85-97.

[4] Charles E. Perkins. Ad Hoc Networking.Addision Wesley, 2001.

[5] C. E. Perkins and P. Bhagwat. Highly dynamic Destination-Sequenced Distance-Vector Routing(DSDV) for mobile computers, ACM Computer Communication Review, Vol. 24, No.4, (ACMSIGCOMM'94) Oct. 1994, pp.234-244.

[6] Charles E. Perkins and Elizabeth M.Royer. "Ad-hoc on-demand distance vector routing". Technicalreport, Sun Micro Systems Laboratories, Advanced Development Group, USA.

[7] Elizabeth M. Royer and Chai-KeongToh. "A review of current routing protocols for ad hoc mobilewireless networks". Technical report, University of California and Georgia Institute of Technology,USA, 1999.

[8] A. S. Tanenbaum, Computer Networks, 3rd ed., Ch. 5, Englewood Cliffs, NJ: Prentice Hall, 1996, pp.357-58.

[9] R. Dube et al., "Signal Stability based Adaptive Routing (SA) for Ad- Hoc Mobile Networks," PerS.Commun., Feb. 1997, pp. 36-45.

[10] C-K. Toh, "Associativity-Based Routing for Ad-Hoc Mobile Networks," Wireless Pers. Commun.,vol. 4, no. 2, Mar. 1997, pp. 1-36.

[11] G. Pei, M. Gerla and T.-W. Chen, Fisheye State Routing in Mobile Ad Hoc Networks. In Proceedingsof the 2000 ICDCS Workshops, Taipei, Taiwan, Apr. 2000, pp. D71-D78

[12] G. Pei, M. Gerla, and X. Hong, LANMAR: Landmark routing for large scale wireless adhocnetworks with group mobility. In Proceedings of the ACM Symposium on Mobile Ad HocNetworking and Computing (MOBIHOC), pages 11-18, 2000.

[13] T.-W. Chen, M. Gerla, Global state routing: a new routing scheme for ad-hoc wireless networks, in:Proceedings of the IEEE ICC, 1998.

[14] V.D. Park, M.S. Corson, A highly adaptive distributed routing algorithm for mobile wirelessnetworks, in: Proceedings of INFOCOM, April 1997.

[15] Krishna Ramachandran, Aodv-st, Technical report, University of California, Santa Barbara, USA.

[16] Mohammed Bouhorma, H.Bentaouit& A. Boudhir, "Performance Comparison of Ad Hoc RouitngProtocols AODV & DSR", IEEE 2009.

[17] R. J. Ramanathan R, "A Brief Overview of Mobile Ad hoc Networks: Challenges and Direction," IEEE Communications Magazine,vol. 40, pp. 20-23, 2002.

[18] Y. Kim, IL. Moon and S. Cho: A Comparison of Improved AODV Routing Protocol Based IEEE802.11 and IEEE802.15.4", Journal of Engineering Science and Technology Vol. 4, No. 2, 2009, pp.132 – 141

Review of Proactive Routing Protocols in Ad Hoc Wireless Networks

Rohit Singhal[1],Vedant Rastogi[2],Sourabh Banga[3]
[1,2]Associate Professor, [3]Assistant Professor
Department of Computer Science, Institute of Engineering & Technology, Alwar, Rajasthan

Abstract

The key challenges in mobile Ad Hoc networks are efficient and dynamic routing. An ad hoc routing protocol is a standard that controls the way computing devices route packets in a mobile ad hoc network. The aim of ad hoc routing protocol is to establish correct and efficient route between pair of nodes that requires minimum overhead and bandwidth consumption. A number of ad hoc routing protocols have been proposed so far. In this article we examine four proactive ad hoc routing protocols-Destination-Sequenced and Distance-Vector (DSDV), Wireless Routing Protocol (WRP), Optimized Link State Routing (OLSR) and Topology Broadcast based on Reverse-Path Forwarding (TBRPF) protocol based on set of performance parameters.

Keywords—DSDV, WRP, OLSR, TBRPF

1 .INTRODUCTION

Wireless network has become very popular in computing industry. Wireless network are adapted to ensure mobility. Mobile Ad Hoc networks[5] are wireless networks which do not require any infrastructure support for transferring packet between two nodes. Communication is directly between nodes or through intermediate nodes acting as routers. Wireless networks are used to augment rather than replace wired networks and are most commonly used to provide last few stages of Connectivity between a mobile user and wired network.

Wireless networks provide connection flexibility between users in different places. Moreover, the network can be extended to any place or building without the need for a wired connection. Wireless networks are classified into two categories: Infrastructure networks and Ad Hoc networks.

Infrastructure Networks: This is infra-structured network (i.e. a network with fixed and wired gateways). An Access Point (AP) represents a central coordinator for all nodes. Any node can be joining the network through AP. In addition, AP organizes the connection between the Basic Set Services (BSSs) so that the route is ready when it is needed. However, one drawback of using an infrastructure network is the large overhead of maintaining the routing tables.

Ad Hoc Networks: Infrastructure less networks have no fixed routers; all nodes are capable of movement and can be connected dynamically in an arbitrary manner. Nodes of these networks function as routers which discover and maintain routes to other nodes in the network. Such a network may operate in standalone fashion, or may be connected to the larger internet.

2. AD HOC NETWORK CHARACTERISTICS

Mobility: nodes can be rapidly repositioned and/or move in ad hoc networks. We can have individual random mobility, group mobility, motion along pre planned routes, etc. The mobility model can have major impact on the selection of a routing scheme and can thus influence performance.

Multi-hopping: a multihop network is a network where the path from source to destination traverses several other nodes. Ad hoc nets often exhibit multiple hops for obstacle negotiation, spectrum reuse, and energy conservation. Battlefield covert operations also favor a sequence of short hops to reduce detection by the enemy.

Self-organization: the ad hoc network must autonomously determine its own configuration parameters including: addressing, routing, clustering, position identification, power control, etc. In some cases, special nodes (e.g., mobile backbone nodes) can coordinate their motion and dynamically distribute in the geographic area to provide coverage of disconnected islands

Energy conservation: most ad hoc nodes (e.g., laptops, PDAs, sensors, etc.) have limited power supply and no capability to generate their own power (e.g., solar panels). Energy efficient protocol design (e.g., MAC, routing,

resource discovery, etc.) is critical for longevity of the mission.

Scalability: in some for wireless "infrastructure" networks scalability is simply handled by a hierarchical construction. The limited mobility of infrastructure networks can also be easily handled using Mobile IP or local handoff techniques. In contrast, because of the more extensive mobility and the lack of fixed references, pure ad hoc networks do not tolerate mobile IP or a fixed hierarchy structure. Thus, mobility, jointly with large scale is one of the most critical challenges in ad hoc design.

Security: the challenges of wireless security are well known - ability of the intruders to eavesdrop and jam/spoof the channel. A lot of the work done in general wireless infrastructure networks extends to the ad hocdomain. The ad-hoc networks, however, are even more vulnerable to attacks than the infrastructure counterparts. Both active and passive attacks are possible. An active attacker tends to disrupt operations (say, an impostor posing as a legitimate node intercepts control and data packets; reintroduces bogus control packets; damages the routing tables beyond repair; unleashes denial of service attacks, etc.). Due to the complexity of the ad hoc network protocols these active attacks are by far more difficult to detect in ad hoc than infrastructure nets. Passive attacks are unique of ad hoc nets, and can be even more insidious than the active ones. The active attacker is eventually discovered and physically disabled/eliminated. The passive attacker is never discovered by the network. Defense from passive attacks require powerful novel encryption techniques coupled with careful network protocol designs.

3. CLASSIFICATION OF ROUTING PROTOCOLS

There are number of routing protocols currently available in ad hoc networks [6]. There is a need for a general technique to classify protocols available. Traditionally classification was done by dividing protocols to table driven and to source initiated. Table Driven routing protocols attempts to maintain consistent up to date routing information for each and every node in the network. These protocols require maintaining a consistent view. The areas in which they differ are the number of necessary routing related tables and the methods by which changes in network structure are broadcast.

A very different approach from table driven routing scheme is source initiated routing. This type of routing creates routes only when needed by the source node. When a node needs a route to a destination, it initiates a route discovery process with in the network. This process is completed once route is found or all possible route permutations has been established, it is maintained by a route maintenance procedure until either the destination becomes inaccessible along every path from the source or until the route is no longer required. This classification is based on to divide protocols according to following criteria, reflecting fundamental design and implementation choices.

Communication model. What is the wireless communication model? Multi or single channel?

Structure. Are all nodes treated uniformly? How are distinguished nodes selected? Is the addressing hierarchical or flat?

State Information. Is network-scale topology information obtained at each node?

Scheduling. Is route information continually maintained for each destination?

This model does not care for if a protocol is unicast, multicast or geocast. Also it does not deal with how links are measures. In order to overcome this, Finnish Defense force navalacademy modified the model by introducing **Type cast** routing and **Cost function** routing.

There are no measures taken to classify the protocols according to power consumption and awareness in routing protocols. In order to overcome this, we add **power aware** routing to this model.

Communication Model:

The routing protocols presently available can be categorized according to communication model to protocols that are designed for multi-channel or single channel. The example of multichannel protocol is clustered Gateway switched routing (CGSR).Single channel presumes one shared media to be used.

Structure:

Routing protocols can be categorized according to structure as:

Uniform routing: In uniform routing, all nodes acts as same manner as that of other nodes. Sending and receiving messages are control in same way by each and every node. No hierarchy is present in network.

Non-Uniform routing: In this type, there is an effort for the limiting of routing complexity by reducing the number of nodes participating in routing computation.

State of Information:

Protocols can be divided according to state of information obtained at each node as under:

Topology Based routing: This maintains a large scale topology information for each node to participating in topology based protocols. The topology based protocols follows the basic principle of link state protocols.

Destination Based routing:

This does not maintain large scale topology information but maintains topology information needed to know the nearest neighbors. i.e., each node exchanges its distance estimates for all network nodes with each of its immediate neighbors.

PROACTIVE ROUTING

Proactive protocols maintain unicast routes between all pairs of nodes regardless of whether all routes are actually used. Therefore, when the need arises (i.e., when a traffic source begins a session with a remote destination), the traffic source has a route readily available and does not have to incur any delay for route discovery. These protocols also can find optimal routes (shortest paths) given a model of link costs.

Routing protocols on the Internet (i.e., distance vector-based RIP and link state-based OSPF) fall under this category. However, these protocols are not directly suitable for resource-poor and mobilead hoc networks because of theirhigh overheads and/or somewhat poor convergence behavior. Therefore, several optimized variations of these protocols have been proposed for use in ad hoc networks. These protocols are broadly classified into the two traditional categories: distance vector and link state. In distance vector protocols, a node exchanges with its neighbors a vector containing the current distance information to all known destinations; the distance information propagates across the network transitively and routes are computed in a distributed manner at each node. On the other hand, in link state protocols, each node disseminates the status of each of its outgoing links throughout the network (typically via flooding) in the form of link state updates. Each node locally computes routes in a decentralized manner using the complete topology information. In the rest of this section, we describe two protocols from each of these categories that have received wide attention.

DISTANCE VECTOR PROTOCOLS

Destination-Sequenced Distance-Vector (DSDV) [1] was one of the earliest protocols developed for ad hoc networks. Primarily design goal of DSDV was to develop a protocol that preserves the simplicity of RIP, while guaranteeing loop freedom. It is well known that Distributed Bellman-Ford (DBF), the basic distance vector protocol, suffers from both short-term and long-term routing loops (the counting-to-infinity problem) and thus exhibits poor convergence in the presence of link failures. Note that RIP is DBF with the addition of two ad hoc techniques (split-horizon and poisoned-reverse) to prevent two hop loops.The main idea in DSDV is the use of destination sequence numbers to achieve loop freedom without any inter-nodal coordination. Every node maintains a monotonically increasing sequence number for itself. It also maintains the highest known sequence number for each destination in the routing table (called “destination sequence numbers”). The distance/metric information for every destination, typically exchanged via routing updates among neighbors in distance-vector protocols, is tagged with the corresponding destination sequence number. These sequence numbers are used to determine the relative freshness of distance information generated by two nodes for the same destination (the node with a higher destination sequence number has the more recent information). Routing loops are prevented by maintaining an invariant that destination sequence numbers along any

Valid route monotonically increase toward the destination.

DSDV also uses triggered incremental routing updates between periodic full updates to quickly propagate information about route changes. In DSDV, like in DBF, a node may receive a route with a longer hop count earlier than the one with the smallest hop count. Therefore, always propagating distance information immediately upon change can trigger many updates that will ripple through the network, resulting in a huge overhead. So, DSDV estimates route settling time (time it takes to get the route with the shortest distance after getting the route with a higher distance) based on past history and uses it to avoid propagating every improvement in distance information.

Wireless Routing Protocol (WRP) [2] is another distance vector protocol optimized for ad hoc networks. WRP belongs to a class of distance vector protocols called path

findingalgorithms. The algorithms of this class use the next hop and second-to-last hop information to overcome the counting-to-infinity problem; this information is sufficient to locally determine the shortest path spanning tree at each node. In these algorithms, every node is updated with the shortest path spanning tree of each of its neighbors. Each node uses the cost of its adjacent links along with shortest path trees reported by neighbors to update its own shortest path tree; the node reports changes to its own shortest path tree to all the neighbors in the form of updates containing distance and second-to-last hop information to each destination.

Path finding algorithms originally proposed for the Internet suffer from temporary routing loops even though they prevent the counting-to-infinity problem. This happens because these algorithms fail to recognize that updates received from different neighbors may not agree on the second-to-last hop to a destination. WRP improves on the earlier algorithms by verifying the consistency of second-to-last hop reported by all neighbors. With this mechanism, WRP reduces the possibility of temporary routing loops, which in turn results in faster convergence time. One major drawback of WRP is its requirement for reliable and ordered delivery of routing messages.

LINK STATE PROTOCOLS

Optimized Link State Routing (OLSR) [3] is an optimized version of traditional link state protocol such as OSPF. It uses the concept of Multipoint Relays (MPRs), discussed in the previous section, to efficiently disseminate link state updates across the network. Only the nodes selected as MPRs by some node are allowed to generate link state updates. Moreover, link state updates contain only the links between MPR nodes and their MPR-Selectors in order to keep the update size small. Thus, only partial topology information is made available at each node. However, this information is sufficient for each to locally compute shortest hop path to every other node because at least one such path consists of only MPR nodes.

OLSR uses only periodic updates for link state dissemination. Since the total overhead is then determined by the product of number of nodes generating the updates, number of nodes forwarding each update and the size of each update, OLSR reduces the overhead compared to a base link state protocol when the network is dense. For a sparse network, OLSR degenerates to traditional link state protocol. Finally, using only periodic updates makes the choice of update interval critical in reacting to topology changes.

Topology Broadcast based on Reverse-Path Forwarding (TBRPF) [4] is a partial topology link state protocol where each node hasonly partial view of the whole network topology, but sufficient to compute as shortest path source spanning tree rooted at the node. When a node obtainssource trees maintained at neighboring nodes, it can update its own shortestpath tree. This idea is somewhat similar to that in path finding algorithms suchas WRP discussed above. TBRPF exploits an additional fact that shortest pathtrees reported by neighbors can have a large overlap. A node can still computeits shortest path tree even if it receives partial trees from each of its neighborsas long as they minimally overlap. Thus, every node reports only a part of itssource tree (called Reported Tree (RT)) to all neighbors in an attempt to reducethe size of topology updates. A node uses periodic topology updates to inform its complete RT to all neighbors at longer intervals, while it uses differential updates to inform them about the changes to its RT more frequently.

In order to compute RT, a node X first determines a Reported Node (RN) set. RN contains itself (node X) and each neighbor Y for which X is on the shortest path to Y from another neighbor. RN so computed contains X and a subset (possibly empty) of its neighbors. For each neighbor Y included in RN, X acts as a forwarding node for data destined to Y. Finally, X also includes in RN all nodes which can be reached by a shortest path via one of its neighbors already in RN. Once X completes computing RN as stated above, the set of all links (u,v) such that u ε RN constitute the RT of X. Note that RT only specifies the minimum amount of topology that a node must report to its neighbors. To obtain some redundancy in the topology maintained at each node (e.g., a sub graph more connected than a tree), nodes can report more topology than RT.

TBRPF also employs an efficient neighbor discovery mechanism using differential hellos for nodes to determine their bidirectional neighbors. This mechanism reduces the size of hello messages by avoiding the need to include every neighbor in each hello message.

4. CONCLUSION

Among the proactive protocols we have discussed, DSDV seems to suffer from poor responsiveness to topology changes and slow convergence to optimal paths. This is mainly because of the transitive nature of topology updates

in distance vector protocols. Simulation results [5] [26] also confirm this behavior. Although reducing the update intervals appears to improve its responsiveness, it might also proportionately increase the overhead leading to congestion. WRP, the other distance vector protocol we have discussed, assumes reliable and in order delivery ofrouting control packets which is anunreasonable requirement in error-prone wireless networks. The performance of the protocol when this assumption does not hold is unclear. As far as the two link state protocols — OLSR and TBRPF — are concerned, both of them share some features such as being partial topology protocols. However, the details of the protocols are quite different. Whereas OLSR is more like a traditional link state protocol with optimizations to reduce overhead in ad hoc networks, TBRPF is a link state variant based on tree sharing concept. TBRPF also has one desirable feature of using frequent incremental updates in addition to periodic, less frequent full updates. This feature will likely improve responsiveness to topology changes. OLSR, on the other hand, relies solely on periodic full updates. Although in our knowledge there is no comprehensive study focusing on relative performance of OLSR and TBRPF, they expected to show comparable performance (and likely better than their distance vector counterparts).

REFERENCES

[1] C. E. Perkins and E. M. Royer. Ad Hoc On-Demand Distance Vector Routing. InProceedings of IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), pages 90–100, 1999.

[2] S. Murthy and J. J. Garcia-Luna-Aceves. An Efficient Routing Protocol for Wireless Networks. ACM/Baltzer Mobile Networks and Applications,1(2): 183–197, 1996.

[3] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum and L.Viennot. Optimized Link State Routing Protocol for Ad Hoc Networks, Hipercom Project, INRIA Rocquencourt, BP 105, 78153 Le ChesnayCedex, France

[4] R. Ogier, M. Lewis, and F. Templin. Topology Dissemination Based on Reverse-Path Forwarding (TBRPF). http://www.ietf.org/internetdrafts /draft-ietf-manet-tbrpf-09.txt, June 2003. IETF Internet Draft (work inprogress).

[5] GeethaJayakumar and G. Gopinath. Ad Hoc Mobile Wireless NetworksRouting Protocols – A Review. In Journal of Science 3 (8) : 574-582, 2007

[6] Beigh Bilal Maqbool and M.A. Meer. Classification of Current Routing Protocols forAd Hoc Networks – A Review. In International Journal of Computer Applications (0975- 8887), Volume 7 – No. 8, October 2010.

Sensing of Selective Forwarding Approaches in Wireless Sensor Networks: A Survey

Ayushi Bhardwaj[1], Anil Rao[2]

[1]M.Tech Scholar, [2]Associate Professor,

Department of Computer Science, Institute of Engineering & Technology, Alwar, Rajasthan

Abstract:

A Wireless Sensor Network (WSN) comprises of disseminated a self-directed devices that monitors both forcible and conditions. Sensor Networks are used for atmospheric condition anticipation and evaluating temperature, sound, wave, vibration, force etc. Sensor Networks suffer from various security approaches like (i) sink hole attack, (ii) black hole attack, (iii) wormhole attack and (iv) selective forwarding attacks. Selective forwarding attack happens in compromised nodes by dropping packets selectively. This paper surveys various techniques for detecting selective forwarding attacks in WSNs.

Keywords: Wireless Sensor Network, Selective Forwarding Attacks, Compromised Nodes, CHEMAS Technique, Lightweight Defense Scheme, and Watermark Technology.

1. Introduction

Wireless sensor network is a self-assembling network of small sensor nodes which conveys with each other using radio signals. WSN brings together sensing, calculation and communication in a single device called as sensor nodes. Wireless sensor nodes are also named as motes. In WSN, sensor nodes are used to send out packets to a base station with the help of multi-hop transmission system.

Sensor nodes are assorted into clusters and each of these clusters has a cluster head, it's shown in Fig1. Through cluster heads, Sensor nodes intercommunicate data to the base station by combining data from its penises [1]. Wireless Sensor Networks are used in sea and wildlife monitoring, constructing machinery performance monitoring, building safety and earthquake monitoring, vehicular movement etc. Due to resource restraints of energy and memory, the conventional security measures are not suitable to these wireless sensor networks. An antagonist can via media a sensor node, it alters the integrity of the data, eavesdrop on messages, inject fake messages, and waste network resources. Unlike wired networks, wireless nodes disseminate their messages to the medium. In wired network, there will not be any security measure problem but not so with Wireless network.Attacks against wireless sensor networks could be broadly considered from two unlike levels of views.

1. The attack versus security mechanisms.
2. The attack versus routing mechanisms.

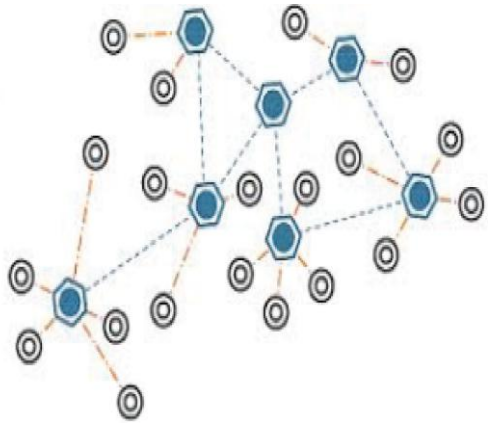


Figure 1: Wireless Sensor Network

Attack Models

Several protection attacks exist in Wireless Sensor Networks and they are,

1. Dos attack
2. Sink hole attack
3. Black hole attack
4. Wormhole attack
5. Selective forwarding attacks.
6. Sybil attacks
7. Sybil attacks
8. Node replication attacks
9. Hello flood attack

The main target of this paper is to give a helicopter view for researchers and developers on different techniques available to keep Selective Forwarding Attack.

2. Selective Forwarding Attack

The selective forwarding Attack was first described by Karlof and Wagner [3]. Selective Forwarding Attack is a network layer attack [2]. In this type of the attack compromised nodes drop particular sensitive messages and forward the rest. It is difficult to identify the compromised node in the whole network.

Selective forwarding attacks are most effective when the attacker is explicitly included on the path of a data flow.

Selective forwarding and black hole attacks are very disastrous attacks for sensor networks if used with sinkhole attack because the intruder can drop most of the important packets. Further classification of this attack is inside attack and outside attack. Inside attack occurs within the network through compromised nodes and outside attack occurs from outside of the network by jamming the communication channels between uncompromised nodes.

2.1 Different Forms of Selective Forwarding Attack

There are different forms of selective forwarding attack.In the First form of the selective forwarding attack, theCompromised node drops some packets. In its Secondform, the Selective forwarding attack behaves like a Blackhole, in which the message is forwards to the wrong path,creating false routing information in the network. Third form of selective forwarding attack delays packet passing through the network creating confused routing information between sensor nodes [3].

3. Related Work

Various techniques are introduced by several researchers to detect malicious nodes that cause selective forwarding attack in Wireless Sensor Networks. These techniques are classified and depicted below in fig 2.

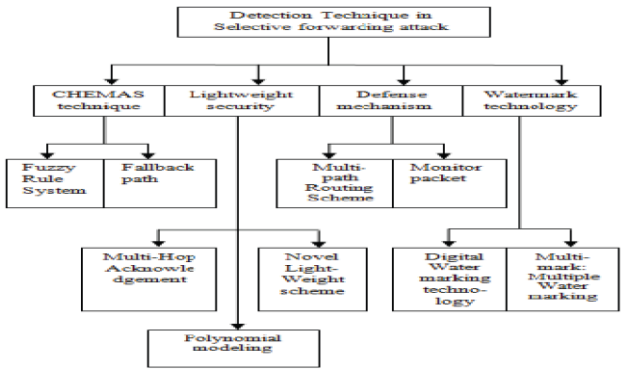


Figure 2: Classification of Selective Forwarding Attack Techniques

3.1 CHEMAS Technique

The Checkpoint Based Multi-hop Acknowledgement Scheme (CHEMAS) was proposed by Bin Xiao et al., to detect selective forwarding attack. When message is generated by a source node and is delivered to the base station, the checkpoint nodes are selected randomly. The base station and each checkpoint nodes generate acknowledgement (ACK) message that is transmitted from the start node to the source node. ACK messages have the Time to Live (TTL) value, which sets the hop count. If TTL becomes zero, ACK message is dropped and an alert message is sent to the source node. If a particular nodedoes not send ACK message to the source then it is identified as the compromised node. Then the source node sends an alarm message about the compromised node to the base station. Ji Won Kim, et al., [5] in their research work, have proposed another technique for the Checkpoint Based Multi-hob Acknowledgement Scheme (CHEMAS) to detect the compromise nodes that perform a selective forwarding attack when sensing data transmission. This paper has achieved a higher detection ratio through each checkpoint node and it generates acknowledgement message to confirm the normal packet. However, if more number of check nodes is presented, then the checking time of the packet transferred will increase and so there will be a time delay in reaching the destination.

Ji Won Kim, et al., [11] in their work, have presented a control method of checkpoint node selection using a fuzzy rule system and feedback in the Checkpoint Based Multihop Acknowledgement Scheme (CHEMAS). The sink node and each checkpoint node generate acknowledgement (ACK) packets to confirm normal packet delivery. If a node has not received sufficient ACK packets, then the nodes generates an alert packet to report the suspect node. Compromised nodes can be detected by analyzing the alert information reported. However, it increases communication.

3.2 Defense Mechanism

Defensive technique for selective forwarding attack consists of three phases for secure information delivery. In first phase the node discovers a path and its neighbor nodes, in second phase, data is propagated in multipath, it checks whether the data received is correct or not, and in the final phase if any error is detected then a MONITOR packet is generated and the malicious node is removed.

Geethu P C and Rameez Mohammed A., [4] in their research work, have described a multipath routing scheme that is used as defense mechanism against selective forwarding attack. When a node detects packet drop during the routing, it will resend the packet through alternate

route, as the resending mechanism reliability of the routing scheme improves then Packet is retransmits through another alternate path. If that path is busy with some other transaction, it leads to time delay and there is a chance for jamming and this is the Limitation of this work.

Pandarinath P., [10] in his research work, has given defensive technique for selective forwarding attack in localization. This technique utilizes secret sharing of information and this information is shared between source and destination using secret sharing algorithm. This algorithm is not suitable for all situations. This algorithm takes more time to execute when more nodes are participating.

ArpitaParida, et al., [6] have introduced a Defensive technique, if any attack is encountered then a monitor packet is generated and subsequently the malicious node is removed. It finds a new path so that the connection will not to be lost and also good delivery ratio can avoid delays. When the path increases, the energy consumption also increases simultaneously.

3.3 Lightweight Defense Scheme

Lightweight security scheme is used to detect selective forwarding attack using multi hop acknowledgement technique. This scheme allows both the base station and source nodes to collect attack alarm information from intermediate nodes. In other words, though the base station is deafened by malicious node the source node can make decisions and responses. The scheme can efficiently obtain those alarm information whenever intermediate nodes in a packet forwarding path detect any malicious packet dropping.

Wang Xin-sheng, et al., [8**]** in their research work, have proposed a light weight defense scheme against selective forwarding attack which uses neighbor nodes as monitor nodes. The neighbor nodes (monitoring nodes) monitor the transmission of packet drops and resend the dropped packets using a hexagonal WSN mesh topology.

Limitation of this paper is that if there is any change in topology, it will affect the performance of the scheme as it is assumed that after development the nodes will not change their location.

Xie Lei et al., [9] in their research work, have described polynomial modeling based on countermeasure against selective forwarding attack and a security scheme using redundant data to tolerate the loss of messages. The basic idea is to split the original data into small parts and forward these parts to the base station. Forwarding nodes cannot understand the contents of the data generated by the polynomial, which can prevent eaves dropping and so sensor nodes in the network cannot be compromised.Finally, before the sensor nodes are deployed, every node shares a unique symmetric key with the base station.

However, dividing and processing the original data packet into small sizes leads to extra storage.

3.4 Watermark Technology

The digital watermarking technology is used to calculate the rate of packets of dropped and modified. Each sensor node can send only a few bits at a time and so the length of watermark embedded into the data should be very short.

The source node generates the watermark W with key K and the feature of the original data. Then the source node embeds the watermark into the original data and transfers it through the media. When the packets reach the Base Station, it the Base Station obtains the feature of the packets and generates the watermark W1 by watermark generation algorithm, then the Base Station extracts the watermark directly from the received packets by Watermark embedding algorithm denoted as W2; finally the packet modified rate is calculate by comparing the W1and W2.

Deng-yin ZHANGa, et al., [7] in their research work, have presented a technique based on digital watermarking technology. This method embeds watermark into the source data packets, and extracted them at the base station without any packet loss. The malicious node prevented from dropping the data. The limitation of this scheme is that it cannot detect more than two malicious nodes on the single path.

Baowei Wang, et al., [12] in their research work, has proposed a novel multiple watermarking methods called Multi-mark. This technique provided privacy, security, and saved storage space and the amount of datatransmitted. Multi-mark is a network structure-free scheme, which can be easily and efficiently applied to the resource limited sensor networks.

4. Future Research Directions

In the existing Defensive proficiency algorithm, a single static path is produced for sending packets to the sink node in the network. When an attack is distinguished, server removes the malicious node and the packets are retransmitted through the new shortest path without losing the connection. This technique can be further enhanced by hiding the packets using the secret sharing algorithm. This approach leads to less conception of energy, good deliverance ratio and avoids delays.

5. Conclusion

The Checkpoint Based Multi-hop Recognition Scheme (CHEMAS) technique is very efficient proficiency for malicious node detection to compare with any other techniques. In CHEMAS, the selection chance of checkpoint is an important factor to determine the security intensity and energy efficiency. The suggested method heightens detection ratio with similar energy consumption to the original CHEMAS scheme. Secure transaction is very difficult in wireless sensor network. This paper studies various efficient detection proficiencies for selective forwarding attack in WSN, aimed by various researchers. This analysis will facilitate to know the drawbacks in the earlier schemes and will help to overcome the withdraws in the future.

References

[1] Jennifer Yick, Biswanath Mukherjee, DipakGhoshal,"Wireless sensor network survey", www.elsevier.com/locate/comnet, April 2008, pp. 2292–2330

[2] Chris Karlof and David Wagner," Secure routing in wireless sensor networks: attacks and countermeasures in Ad Hoc Networks", www.Elsevier.com, Vol.1 No.2, September 2003, pp.293–315.

[3] WazirZadaKhana, Yang Xiangb, Mohammed Y Aalsalem,QuratulainArshad," The Selective Forwarding Attack in Sensor Networks: Detections and Countermeasures" International Journal of Wireless and Microwave Technologies (IJWMT), Vol.2, No.2**,** April 2012, pp.33-44.

[4] Geethu P C and Rameez Mohammed A, "Defense Mechanism against Selective Forwarding Attack in Wireless Sensor Networks", Conference on Computing, Communications and Networking Technologies (ICCCNT), July 2013, pp. 1-4

[5] Ji Won Kim, Soo Young Moon, Tae Ho Cho, Jin Myoung Kim, Seung Min Park, "Improved Message Communication Scheme in selective forwarding attack detection method", Digital Content, Multimedia Technology and its Applications

(IDCTA), 7th International Conference, August 2011, pp.169-172.

[6] ArpitaParida, NachiketaTarasia, TulasiAmbashaPatnaik, "Security against Selective Forward Attack in Wireless Sensor Network**"**, IOSR Journal of Engineering, Vol. 2(5), May 2012, pp. 1200-1206[7] Deng-yin ZHANG, Chao Xu, Lin Siyuan," Detecting selective forwarding attacks in WSNs usingwatermark", Wireless Communications and Signal Processing (WCSP), International Conference, Nov 2011, pp. 1 - 4

[8] Wang Xin-sheng, Zhan Yong-zhao, XiongShu-ming, Wang Liang-min, "Lightweight Defense Scheme against Selective Forwarding Attacks in Wireless Sensor Networks" Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC '09. International Conference, Oct 2009, pp.226-232

[9] Xie Lei, Xu Yong-jun, Pan Yong, Zhu Yue-fei, "A Polynomial based Countermeasure to Selective Forwarding Attacks in Sensor Networks", Commmunications and Mobile Computing, CMC '09. WRI International Conference, Vol.3, Jan 2009, pp.455- 459

[10] Pandarinath P, "Secure Localization with Defense against Selective Forwarding Attacks in Wireless Sensor Networks", Electronics Computer Technology (ICECT), 3rd International Conference, Vol.5, April 2011, pp.-112-116.

[11] Ji Won Kim, Soo Young Moon, Tae Ho Cho, Jin Myoung Kim, Won Tae Kim, Seung Min Park, "Control Method of Checkpoint Node Selection Using a Fuzzy Rule System and Feedback in CHEMAS" Advanced Communication Technology (ICACT), 13th International Conference ,Feb 2011, pp.584-587

[12]Baowei Wang, Xingming Sun, ZhiqiangRuan, HengRen**, "**Multi-mark: Multiple Watermarking Method for Privacy Data Protection in Wireless Sensor Networks", Information Technology Journal, Vol. 10, Issue 4, April 2011, pp.833-840

Shape Representation for Image Retrieval

Komal Vijay[1], Pratap Singh Patwal[2] , Antim Yadav[3]
[1]M.Tech Scholar, [2]Associate Professor, [3]M.Tech Scholar
Department of Computer Science, Institute of Engineering & Technology, Alwar, Rajasthan

Abstract

Vision which is our most significant sense, it gives rise to efforts to Empower computers to represent, process, understand, and act on visual imagery. Images are being generated at a mind-boggling pace from a variety of sources. aerial imagery, surveillance images, mug shots, fingerprints, trademarks and logos, images from sports events, documentation of environmental resources in the form of images, and entertainment industry photos and videos, graphic illustrations, engineering line drawings, documents, manuals, medical images, these are the form in which Terabytes of data are being generated. The management of such databases must rely on the perceptual and cognitive dimensions of the visual space, namely, color, texture, shape, and so on. There exists qualitative aspects of images that can be used to retrieve images without fully specifying them, this is the basic premise.

Keywords: Image Retrieval, Indexing, Shape Similarity, Matching, Validation

1. INTRODUCTION

The use of color or texture is more developed and the use of shape as a cue is less developed mainly because of the inherent complexity of representing it. In many application fields, retrieval-by shape has the potential of being the most effective search technique. The main question is that how to complete or partial information regarding a shape in an image can be represented so that it can be easily extracted, matched, and retrieved. These five key items must be addressed:

Image and Query Preparation: How are shape extracted from images? A wide spectrum of shape-extraction techniques have been developed, ranging from segmenting the image to extracting related lower level features, such as edges, that yield a partial representation of shape. The query-specification mechanism provided by the user interface must closely match the shape extraction process, and, in particular, emphasize the specific representation of shape used during the search.

Shape Representation: How is shape represented? Is the representation contour-based or region based? Is there "invariance" to a class of transformations? Is it based on local features or global attributes?

Shape Similarity and Matching: How are the query and database items matched? How is the similarity between two objects represented?

Indexing and Retrieval: How is the database organized?

Validation: How efficient is the retrieval?

2. WHERE IS INDEXING BY SHAPE RELEVANT?

It is inherently difficult to characterize and manipulate, shape is a significant cue for describing objects. An increasing number of applications have used it as a primary cue for indexing, a few of which are here:

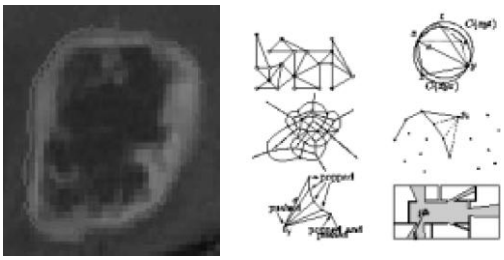
By their specific shapes, Trademarks and logos are often distinguished. By checking the similarity in shape with previously used forms, Patent application offices must avoid duplication partly

Shape is used as a cue to describe the similarity of medical scans, in the medical domain. Several image query systems supporting retrieval-by-shape have been developed.

In the management of document databases, Shape also plays a key role. Sample applications include the retrieval of architectural drawings, technical drawing of machine parts, clipart, and graphics.

Another application area for retrieval of images by shape is Law-enforcement and security. In automatic personal identification for criminal identification by law-enforcement agencies, access control to restricted facilities, credit card user identification, and other applications, Fingerprint matching is used.

Earth Science applications of retrieval-by-shape include indexing databases of auroras.



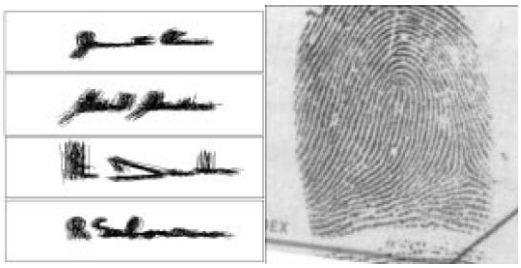


Figure 1: Examples of shapes for indexing into a database: medical structures, drawings, fingerprints and signatures.

Art and art history, multimedia systems for museums and archaeology, defense, electronic shopping and entertainment are other applications.

3. IMAGE PREPARATION AND QUERY FORMULATION

A complete representation of a two-dimensional shape is provided by its contour. A continuous curve in the plane is contour. And can specify by a large number of points. for similarity retrieval such a voluminous representation of shape cannot be effectively used, partial representations capturing its salient aspects are used in practice Range of these partial representations are from very simple to very complex.

The image must be segmented and entire shapes must be stored, when a complete description of shape is used in the indexing scheme. When images contain binary or nearly binary shapes, such as trademarks, logos, bitmaps of characters, signatures, clip art, designs, drawings, graphics, and so on, this process is quite straightforward. In general, however, the task of figure-ground segregation is formidable, as is evident from the relatively large "segmentation" literature in computer vision and image processing. Nevertheless, in certain domains automatic segmentation has been used. For example, Gunsel and Tek alp address the segmentation, or figure background separation problem, by a combination of methods. A color histogram intersection method is used to eliminate database objects with significantly different color from the query object. Boundaries are estimated using either the canny edge detector or the graduated nonconvexity (GNC) algorithm.

Partial representations are often used when application requirements permit. The most common methods rely on edge content, which is indicative of shape boundary. A brief historical sequence that samples these methods is presented here.

A pixel-by-pixel edge-content comparison of a query, Hirata and Kato performed and shifted image blocks and used the resulting "edge similarity score" to find the best match. This approach is evaluated by Gray. He concluded that its fundamental weakness is the "pixel-by-pixel" nature of the comparison, which produces multiple false matches. The notion of flexible matching for indexing is introduced by DelBimbo, which allows for significant deviations of the sketch from the edge map. Chan and coworkers extend the pixel-by-pixel approach to correlation of "curvelets" by grouping edge pixels into edge elements using the Hough transform, by modeling grouped edges as curvelets using implicit polynomial (IP) models, and by computing the similarity between a pair of IP curvelets.

4. REPRESENTATION OF SHAPE

Shape has been represented using a variety of descriptors such as moments, geometric and algebraic invariants, polygons, polynomials, splines, strings, Fourier descriptors (FD), deformable templates, skeletons, and so on, for both object recognition and for indexing of image databases.

Shape comparison is also a very difficult problem. The key observation is that shape, a construct of the projected object that is a perceptual invariant of the object, is multifaceted.

Boundary Versus Interior

Two large categories of shape descriptors can be identified: those capturing the boundary (or contour appearance) and those characterizing the interior region. A boundary can be described by its features, for example, curvature extrema and inflection points. The interior has been modeled in a variety of ways, including collections of primitives, deformable templates, by modes of resonance, skeletal models, or simply as a set of points.

Boundary-based or region-based, each representation is intuitively appealing and corresponds to a perceptually meaningful dimension. Each representation can be used as a basis to compute the other that is, by filling in the interior region or by tracing the boundary.

Local Versus Global

Shape can also be viewed either from a local or from a global perspective. Many early models in indexing by shape content used features such as moments, eccentricity, area, and so on, which are typically based on the entire shape and are thus global. Similarly, Fourier descriptors of two-dimensional shape are global descriptors. On the other hand, local representations restrict computations to small neighborhoods of the shape.Purely global representations are affected by variations, such as partial occlusion and articulation, whereas purely local representations are sensitive to noise.

Composition of Parts Versus Deformation

Shape can also be viewed either as the composition of simpler, elementary parts, or as the deformation of simpler shapes. Shapes are composed of simple components, in the "part-based view". The partitioning can be based on either global fit or local evidence. Shape can also be decomposed into parts based on "local" evidence. Properties of the boundary belong to this category.Where shape variability is captured by allowable transformations of a template is the representation of Deformable templates. Generally, two forms of deformable shape models have been proposed, which differ, based on whether the model itself or the deformation of the model is parameterized.

Scale: Coarse to Fine

Shape can be represented along a range of scales spanning coarseto fine. The first type of scale-spaces description of shape was based on linear operators, such as Gaussian scale space. Mokhtarian and coworkers represent shape by two vectors corresponding to boundary coordinates (x and y). The shape is reconstructed from the smoothed boundary coordinate vectors and each vector is smoothed by Gaussian smoothing. "Curve shortening flow" is a geometric smoothing method in which each point of a curve moves along its normal proportional to the signed curvature. The mathematical morphology framework considers shape as a set of (interior) points that are simplified by "closing" and "opening" operations which is the alternative to these boundary-based scale-space representations of Shape.

Partial or Complete

Complete representation of shape retains all the information necessary to reconstruct the shape while Partial representation of shape retains only those features that are most useful for distinguishing a pair of shapes in a database of interest and ignores other features.

Coverage and Denseness

Coverage is the extent to which a representation describes arbitrary shapes, that is, it is a measure of the size of the class of shapes perfectly captured by the representation. A dense representation closely approximates every shape to any desired accuracy.

Isolated Shape and Shape Arrangements

A shape representation can focus on individual objects independently, or it can also include their spatial arrangement.

5. MATCHING, SHAPE SIMILARITY, AND VALIDATION

In an indexing scheme, the type of shape representation has significant implications for the matching process, and vice-versa. A rich representation allows for robust comparison with relatively less effort whereas A poor representation, namely, one in which relevant variations in shape do not translate to variations in the representation, relegates much of the effort of accounting for variation to the matching process. Ideally, the representation should map each shape to a vector of numbers in such a way that the Euclidean distance between pairs of vectors indicates shape dissimilarity. Two matching procedures are Boundary-based technique and region-based technique. Boundary-based techniques are typically accompanied by curve-based comparisons. In these approaches two curves are compared based on their properties, such as curvature, resulting in a single similarity measure. Alternatively, region-based representations typically involve trees and have relied on such methods as graph-tree matching, string edit distance, graduated assignment, tree edit distance, eigenvalue decomposition, Bayesian matching, containment tree matching, and so on. Modal matching and deformable prototypes are some other region-based techniques which allows for a global to local ordering of shape deformations.

6. Conclusion

In many application fields, retrieval-by shape has the potential of being the most effective search technique. Shape has been represented using a variety of descriptors for both object recognition and for indexing of image database. Each of these representations aims at capturing specific perceptually salient dimensions of the qualitative aspects of shape. The type of shape representation has significant implications for the matching process.

References

[1].V.N. Gudivada and V.V. Raghavan, Content-based image retrieval systems, IEEE Comput. **28**, 18–22 (1995).

[2].R. Mehrotra and J.E. Gary, Similar shape retrieval in shape data management, Comput. **28**(9), 57–62 (1995).

[3].V.E. Ogle and M. Stonebraker, Chabot: retrieval from a relational database of images, Comput. **28**(9), 40–48 (1995).

[4].M. Flicknet et al., Query by image and video contact: the QBIC system, Computer **28**(9), 23–31 (1995).

[5].A.D. Narasimhalu, M.S. Kankanhali, and J. Wu, Benchmarking multimedia databases, Multimedia Tools Appl. **3**(4), 333–355 (1997).

[6].W.I. Groski and R. Mehrota, Index-based object recognition in pictorial data management, Comput. Vis. Graphics, Image Process. **52**, 416–436 (1990).

[7]. Ralescu and R. Jain, Special issue on advances in visual information management systems, J. Intell. Inf. Syst. **3** (1994).

[8].J.P. Eakins, Retrieval of trade-mark images by shape feature, Proceedings of First International Conference on Electronic Library and Visual Information Research,DeMontfort University, Milton Keynes, May 3–5 1994.

[9].J.P. Eakins, K. Shields, and J. Boardman, ARTISAN—a shape retrieval system based on boundary family indexing, Proc. SPIE **2670**, 17–28 (1996).

[10]. Shields, J.P. Eakins, and J.M. Boardman, Automatic image retrieval using shape features, New Rev. Doc. Text Manage. **1**, 183–198 (1995)

Study of Mobility Models for Ad Hoc Networks

Ruchika[1],Mohit Khandelwal[2]

[1]M.Tech Scholar, [2]Associate Professor,

Department of Computer Science, Institute of Engineering & Technology, Alwar, Rajasthan

ABSTRACT

An ad hoc network is an aggregation of wireless nodes forming a provisional network without any established and central infrastructure. Mobile Ad-hoc Network (MANET) is an infrastructure less and decentralized network which need a robust dynamic routing protocol. Routing protocols helps node to send and receive packets. Routing is a challenging issue in MANET. A mobile system is characterized by the movement of its constituents. The mobility model is designed to describe the movement pattern of mobile users, and shows how their location, velocity and acceleration changes over time. Mobility patterns used to determine the protocol performance. The study of Mobility Models and their realistic vehicular model deployment is a challenging task. It tries to illustrate the behavior of a real world object.

Keywords: AOD, DSR, RWP, RPGM.

1. INTRODUCTION

In the past few decade the field of wireless network have become very popular. In wireless networks computers are connected and communicate with each other not by a visible path, but by an emission of electromagnetic energy in the air. Recently Wireless LANs are being deployed on airports and conferences etc. People have started using different portable devices to access Internet and other resources using wireless networks while moving. Another area which has generated a lot of interest recently, is wireless ad-hoc networks [1]. Wireless networking is an emerging and increasingly popular technology that allows users to access information and services electronically, notwithstanding of their geographic positions.In the following sections we will have literature survey of the work followed by the discussion on the Performance of AODV and DSR routing protocol with different mobility models.

2. LITERATURE REVIEW

Extensive research has been done in modeling mobility for MANETs. In this section, we mainly focus on experimental research in this area. **ZuraidaBinti et al.[2]**The major requirements of a routing protocol was proposed by that includes minimum route acquisition delay, loop-free routing, quick routing reconfiguration, minimum control overhead, distributed routing approach, and scalability. However, there is a severe lacking in implementation and operational experiences with existing MANET routing protocols. Various types of mobility models were identified and evaluated by**Tracy Camp et al. [3]** and it is seen that the mobility of a node will also affect the overall performance of the routing protocols.

3. MOBILITY MODELS

A mobility model [3] defines the rules that can be used to generate trajectories for mobile nodes.

Mobility models are based on setting out different parameters related to node movement. Mobility models are used in simulation studies to describe the dynamic behaviors of mobile devices in the real world for analyzing and evaluating the performance of ad hoc network protocols under various scenarios [3]. Mobility models play a significant role in the development of MANETs. Currently, in the literature [3] there is a lot of mobility models used, mostly in simulations.

Mobility model identifies the primary place of nodes and the manner of node mobility. The mobility models fall into two categories: one is realistic and other is unrealistic. The realistic mobility models are similar to the real world conditions, they provide more accurate results. The most important characteristic of a mobility model is the degree of realism with respect to the movement of users in real life.

- **Existing Mobility Models**

This section presents a comprehensive evaluation of existing mobility models for an ad-hoc network. A mobility model should attempt to mimic the movements of realistic MNs. Changes in speed and direction must occur with time slots. Currently there are two types of mobility models used in simulations of ad hoc networks: trace based mobility models and synthetic models.

- **Trace Based Mobility Models**

Traces are those mobility patterns that are observed in real life scenarios. Traces provide accurate information, specifically when they involve a large number of participants and an appropriately long observation period. It also gives a realistic measurement of user's behavior in wireless network environments. For example, "re-play" the trace as a mobility input for users in the simulation.

- **Synthetic Mobility Models**

Until a trace has not been created a new network environment (e.g. ad hoc networks) have not easily modeled. In this situation it is necessary to use synthetic models. Synthetic models represent the movements of the mobile nodes without using mobility traces. Synthetic models attempt to realistically represent the behaviors of mobile nodes (MNs) without the use of traces. In this paper, we present various synthetic mobility models that have been proposed (or used in) to evaluate the performance of ad hoc network protocols [8].

In mobile ad hoc networks, there exist many situations where the movements of mobile nodes have some correlation with each other, i.e. mobile nodes have some group behavior in common. The Group Models have been proposed to present this characteristic. Most of MANET simulations are based on random mobility models used to generate network topology changes due to node movement. Thus, apart from the Random Waypoint model, we use the following mobility models:
1) Reference Point Group Mobility (RPGM) Model
2) Manhattan Mobility Model

- **Random way point mobility model**

The Random waypoint model was first proposed by Johnson and Maltz. Random Waypoint (RWP) model is often used synthetic model for mobility, for e.g., in Ad Hoc networks. It is an elementary model which describes the movement patterns of independent nodes by simple terms [9].

The Random waypoint model is a random model for the movement of mobile users, and shows how their location, velocity and acceleration change over time. The random way point model is the simplest model but still the most widely used model to evaluate the performance of MANETs. The random way point model includes pause time between changes in direction and/or speed. In random-based mobility model simulations, mobile nodes move freely and randomly without any restrictions. Briefly, in the RWP model:

- Each node moves along a zigzag line from one waypoint P_i to the next P_{i+1}.
- The waypoints are uniformly distributed over a convex area.
- At the starting point of each leg a random velocity is drawn from the velocity distribution.

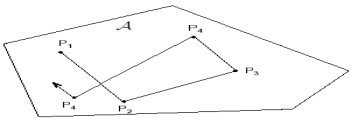


Fig 1: Random Way Point Model

As a Mobile Node begins to move, it stays in one location for a certain period of time i.e. pause time. Once the pause time is elapsed, the Mobile node randomly chooses the next destination in the simulation area and selects a random speed uniformly distributed between [minspeed, maxspeed] and travels with a speed v which is uniformly chosen between the interval (0, Vmax). Then, the MN continues its journey toward the newly selected destination at the chosen speed. As the mobile node arrives at the destination, it stays again for the specified pause time before continuing the process.

However, since the behavior of this model is independent of past motion (memoryless), means it generates very unrealistic displacements. Figure shows the travelling pattern followed by a node in RWP model.

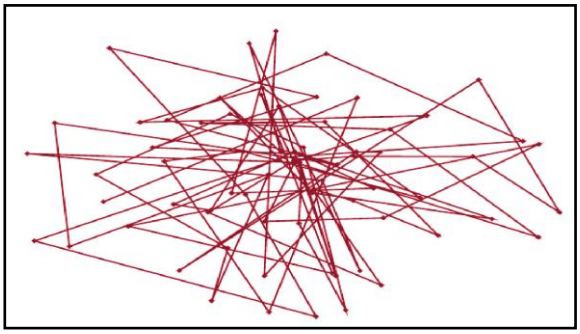


Fig. 2: Travelling pattern using Random Way Point Model

The mobility of RWP constantly causes topology change. The Random Waypoint Mobility Model is widely used in simulation studies of MANET.

- **Reference Point Group Mobility Model**

Reference Point Group Mobility Model [3,4] (RPGM) described as another way to simulate group behavior. In reference point group mobility model, each node belongs to a group where every node follows a logical centre (group leader) that determines the group's motion behavior. Group movements are based upon the path travelled by a logical

centre for the group. The movement path of a group is predefined by a series of points, which are referred to as "reference points".

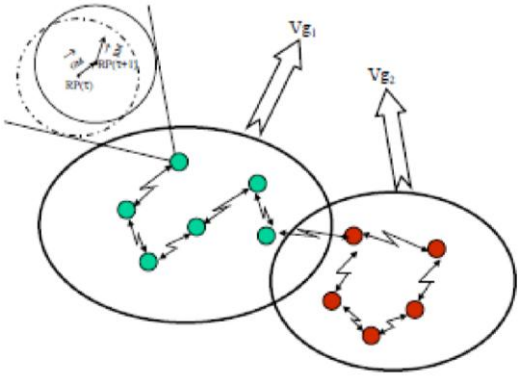


Fig. 3: Group mobility model

Fig gives an example of a two-group model. Each group has a group motion vector GM. The figure also gives an illustration of how a node moves from time tick t to (t+1) First, the reference point of a node moves from RP(t) to RP(t+1)with the group motion vector GM [10]. The nodes in a group are randomly distributed around a reference point. Each node uses their own mobility model and is then combined to the reference point, which directs them in the direction of group. It is used to calculate group motion via a group motion vector, GM (here $GM=V_{gi}$). The motion of the group centre completely characterizes the movement of this corresponding group of mobile nodes including their direction and speed. An individual mobile node moves randomly and freely about their own pre-defined reference points whose movements depend on their group movement. As long as the individual reference point move from time t to t+1, their locations are updated according to the group's logical centre [10]. Once the updated reference group points, RP (t+1) are calculated, they are combined with a random vector, RM, to show the random motion of each mobile node about its individual reference point. The overall length of RM is uniformly distributed within a specified radius cantered at RP (t+1) and its direction is uniformly distributed between 0 and Pi. This model adds two columns in the trace files: "Group Number" tells group number of the node, and "Is Leader" shows if the corresponding node is the leader of its group.

- **Manhattan Grid Mobility Model**

The Manhattan grid model [3] used to emulate the movement pattern of mobile nodes on streets defined by maps. The Manhattan mobility model uses a grid road topology. This model was mainly proposed for the movement in an urban area, where the streets are in an organized and ordered manner. The Manhattan map used in our study is shown in Fig.5

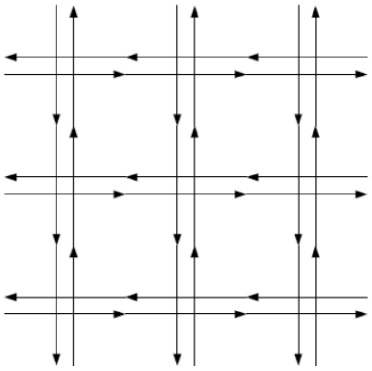


Fig 5: Manhattan grid Map

The map is composed of a number of horizontal and vertical streets. Every street has two lanes in each direction (North and South direction for vertical streets and East and West for horizontal streets). The mobile nodes are assumed to be randomly placed in the street intersections. The movement of a node is decided one street at a time. The Manhattan model employs a probabilistic approach in the selection of nodes movements, at an intersection of a horizontal and a vertical street. Each mobile node can turn left, right or goes straight [7]. This choice is probabilistic: the probability of moving on the same street is 0.5(half), the probability of turning into left is 0.25 and the probability of turning into right is 0.25. The current velocity of a mobile node at a time slot is dependent on its velocity at the previous time slot. Here a node velocity is restricted by the velocity of the node preceding it on the same lane of the street.

Applications: It can be useful in modeling movements in an urban area where a pervasive computing service between portable devices is provided.

Important Characteristics of Manhattan Mobility model:

- The mobile node in Manhattan model is allowed to move along the grid of vertical and horizontal streets on the map.
- At an intersection point of a horizontal and a vertical street, each mobile node can turn to left, right or go straight with definite probability.
- Except the above mentioned difference, the property of inter-node and intra-node relationships involved in this model is same as in the Freeway model.

4. CONCLUSION

Every model mentioned above could be used to model the mobility of mobile node in MANET. They may be used in some particular situations, but none of them is flexible and suitable enough for modeling more realistic scenarios. The Entity Models and the Group Models can co-exist in some scenarios.

REFERENCES

[1] DimitriBertsekas and Robert Gallager, "Data Networks- 2nd Edition", Prentice Hall, New Jersey, ISBN 0-13-200916-1.

[2] ZuraidaBinti Abdullah Hani and Mohd.Dani Bin Baba, "Designing Routing protocols for Mobile Ad hoc networks",IEEE 2003.

[3] Tracy Camp, Jeff Boleng and Vanessa Davies, " A Survey of Mobility Models for Ad Hoc Networks Research", Wireless Communication & Mobile Computing (WCMC): Special issue on Mobile Ad Hoc Networking:Research, Trends and Applications, vol. 2, no. 5, pp. 483-502, 2002.

[4] Birdar, S.R.; Sarma, H.H.D.; Sharma, K.; Sarkar, S.K.; Puttamadappa, C., " Performance Comparison of Reactive Routing Protocols of MANETs Using Group Mobility Model" in proc. IEEE International Conference on Signal Processing Systems, Page(s): 192 – 195, 2009.

[5] Azizol Abdullah, NorlidaRamly, Abdullah Muhammed, Mohd Noor Derahman "Performance comparison study of Routing Protocols for Mobile Grid Environment", IJCSNS International Journal of Computer Science and Network Security, Vol. 8, No 2, February 2008, pp 82-88.

[6] Sachin Kumar Gupta and R.K.Saket, " Routing Protocols in Mobile Ad hoc Networks", IJCA special issue on ICEICE, Number 4, pp 24-27,

[7] December 2011, Published by Foundation of Computer Science, New York, USA.

[8] G. Jayakumar, G. Gopinath, "Performance Comparison of MANET Protocol Based on Manhattan Grid Model", Journal of Mobile Communications, vol. 2, no. 1, pp. 18-26, 2008.

[9] Kapang Lego, Pranav Kumar Singh, DipankarSutradhar, "Comparative Study of Adhoc Routing Protocol AODV, DSR and DSDV in Mobile AdhocNETwork", Indian Journal of Computer Science and Engineering Vol. 1 No. 4 364-371, 2011.

[10] Meetasingh et al. "Performance Evaluation of AODV and DSR using Random Way Point Mobility Model", International Journal of Computer Applications (0975 – 8887) Volume 46– No.19, May 2012.

[11] KavitaPandey, AbhishekSwaroop, "A Comprehensive Performance Analysis of Proactive, Reactive and Hybrid MANET Routing Protocols", International Journal of Computer Science Issues, Vol. 8, Issue 6, No 3, November 2011

A Survey on Location Hiding & Security Observations in Local Area Wireless Sensor Network

Bhanu Pratap Singh[1],Rohit Singhal[2],Monika Yadav
[1]M.Tech Scholar, [2]Associate Professor,
Department of Computer Science, Institute of Engineering & Technology, Alwar, Rajasthan

Abstract

Location Monitoring Systems when send a personal location data to untrusted server, it may pose a privacy threat to the monitored objects. A 2D privacy preserving location monitoring system for wireless sensor networks is used to preserve the privacy of monitored objects in single floor-multi section building and to provide the monitoring services to the system users.

In this system, two location anonymization algorithms, namely, 2D recourses-aware and 2D quality-aware algorithms are used. Using these algorithms the system is able to provide high quality location monitoring services for system users, while preserving personal location privacy. Both algorithms uses well established k-anonymity privacy concept to preserve the privacy of monitored objects. By using these algorithms the sensor nodes can provide the aggregate location information of monitored persons to the containment resolver which after resolving containment sends this aggregate location information to the server. Each aggregate location is in a form of a 2D monitored area A along with the number of monitored persons residing in A, where A contains at least k persons.

The 2D resource-aware algorithm minimizes communication and computational cost, while the 2D quality-aware algorithm is used to maximize the accuracy of the aggregate locations by minimizing their monitored areas. To utilize the aggregate location information to provide location monitoring services, we use a 2D spatial histogram approach that estimates the distribution of the monitored persons in singlefloor-multisection building. Then the estimated distribution is used to provide location monitoring services through answering range queries

.Keywords— Location privacy, wireless sensor networks, location monitoring system, aggregate query processing, spatial histogram..

1. INTRODUCTION

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on [2].

The WSN is built of ”nodes” from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy existence, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning ”motes” of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on existences such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

Characteristics of WSN

- Power consumption constrains for nodes using batteries or energy harvesting
- Ability to cope with node failures
- Mobility of nodes
- Communication failures
- Heterogeneity of nodes
- Scalability to large scale of deployment
- Ability to withstand harsh environmental conditions
- Ease of use

2. PRIVACY PRESERVATION IN LOCATION BASED WSN

The advance in wireless sensor technologies has resulted in many new applications for military and/or civilian Purposes. Many cases of these applications rely on the information of personal locations, for example, surveillance And location systems. These location-dependent systems are realized by using either identity sensors or counting Sensors. For identity sensors, for example, Bat and Cricket, each individual has to carry a signal sender/ receiver unit with a globally unique identifier. With identity sensors, the system can pinpoint the exact location of each monitored person.

On the other hand, counting sensors, for example, photoelectric sensors and thermal sensors, are deployed to report the number of persons located in their sensing areas to a server[7].

Unfortunately, monitoring personal locations with a potentially untrusted system poses privacy threats to the monitored individuals, because an adversary could abuse the location information gathered by the system to infer personal sensitive information. For the location monitoring system using identity sensors, the sensor nodes report the exact location information of the monitored persons to the server; thus using identity sensors immediately poses a major privacy breach. To tackle such a privacy breach, the concept of aggregate location information, that is, a Collection of location data relating to a group or category of persons from which individual identities have been removed, has been suggested as an effective approach to preserve location privacy. Although the counting sensors by nature provide aggregate location information, they would also pose privacy breaches. Fig. 1 gives an example of a rivacy breach in a location monitoring system with counting sensors. There are 11 counting sensor nodes installed in nine rooms R1 to R9, and two hallways C1 and C2 (Fig. 1a). The nonzero number of persons detected by each sensor node is depicted as a number in parentheses. Figs. 1b and 1c give the numbers reported by The same set of sensor nodes
at two consecutive time instances ti1 and ti2, respectively. If R3 is Alices office room, an adversary knows that Alice is in room R3 at time ti. Then, the adversary knows that Alice left R3 at time ti1 and went to C2 by knowing the number of persons detected by the sensor nodes in R3 and C2.

Likewise, the adversary can infer that Alice left C2 at time ti2 and went to R7. Such knowledge leakage may lead to several privacy threats. For example, knowing that a person has visited certain clinical rooms may lead to knowing the her health records. Also, knowing that a person has visited a certain bar or restaurant in a mall building may reveal confidential personal information.

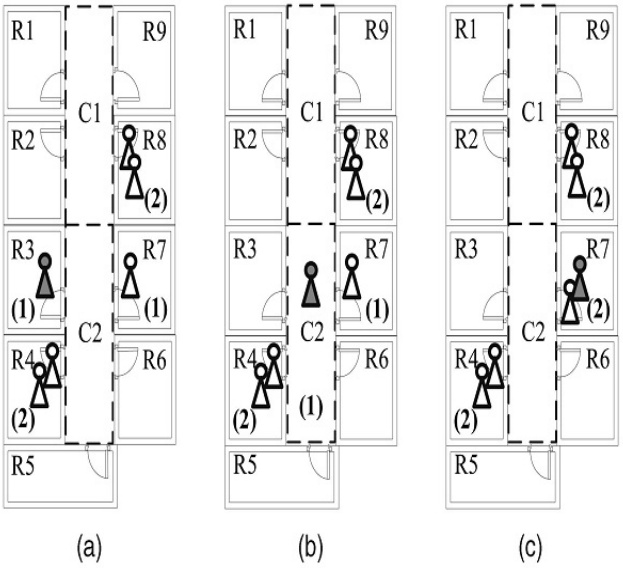


Fig -A location monitoring system using counting sensors. (a) At time ti. (b) At time ti+1**.**

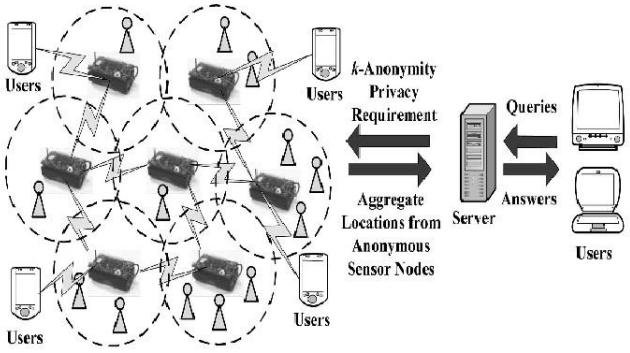


Fig : System Architecture

Sensor nodes

Each sensor node is responsible for determining the number of objects in its sensing area, blurring its sensing area into a cloaked area A, which includes at least k objects, and reporting A with the
number of objects located in A as aggregate location information to the server. We do not have any assumption about the network topology, as existing system only requires a communication path from
each sensor node to the server through a distributed tree [10]. Each sensor node is also aware of its location and sensing area.

Server

The server is responsible for collecting the aggregate locations reported from the sensor nodes, using a spatial histogram to estimate the distribution of the monitored objects, and answering range queries based on the estimated object distribution. Furthermore, the administrator can change the anonymized level k of the system at anytime by disseminating a message with a new value of k to all the sensor nodes.

System users

Authenticated administrators and users can issue range queries to existing system through either the server or the sensor nodes, as depicted in Fig. 2. The server uses the spatial histogram to answer
their queries.

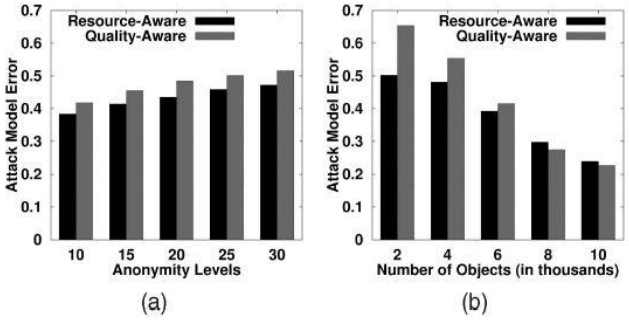
Privacy model

In this system, the sensor nodes constitute a trusted zone, where they behave as defined in existing algorithm and communicate with each other through a secure network channel to avoid internal network attacks, for example, eavesdropping, traffic analysis, and malicious nodes. Since establishing such a secure network channel has been studied in the literature, the discussion of how to get this network channel is beyond the scope of this paper. However, the solutions that have been used in previous works can be applied to existing system. Existing system also provides anonymous communication between the sensor nodes and the server by employing existing anonymous communication techniques. Thus given an aggregate location R, the server only knows that the sender of R is one of the sensor nodes within R. Furthermore, only authenticated administrators can change the k-anonymity level and the spatial histogram size. In emergency cases, the administrators can set the k-anonymity level to a small value to get more accurate aggregate locations from the sensor nodes, or even set it to zero to disable existing algorithm to get the original readings from the sensor nodes, in order to get the best services from the system. Since the server and the system user are outside the trusted zone, they are untrusted.

3. EXISTING WORK RESULT ANALYSIS

Anonymization Strength

Fig. 3 depicts the resilience of existing system to the attacker model with respect to the anonymity level and the number of objects. In the figure, the performance of the resource and quality-aware algorithms is represented by black and gray bars, respectively. Fig. 7a depicts that the stricter the anonymity level, the larger the attacker model error will be encountered by an adversary. When the anonymity level gets stricter, existing algorithms generate larger cloaked areas, which reduce the accuracy of the aggregate locations reported to the server. Fig. 7b shows that the attacker model error reduces, as the number of objects gets larger. This is because when there are more objects, existing algorithms generate smaller cloaked areas, which increase the accuracy of the aggregate locations reported to the server. It is difficult to set a hard quantitative threshold for the attacker model error.
However, it is evident that the adversary cannot infer the number of objects in the sensor nodes sensing area with any fidelity.**Effect of Query Region Size**



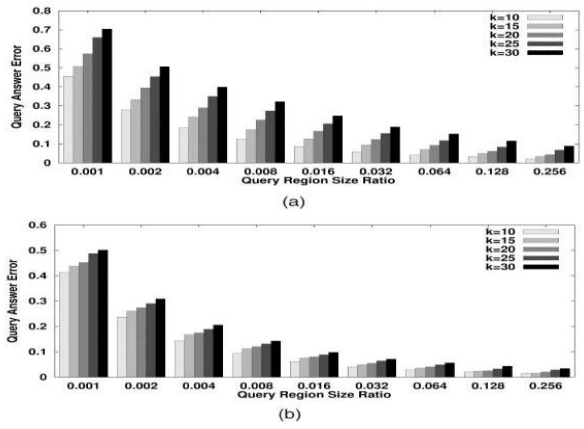
Fig

Fig. 3 depicts the privacy protection and the quality of existing location monitoring system with respect to increasing the query region size ratio from 0.001 to 0.256, where the query region size ratio is the ratio of the query region area to the system area and the query region size ratio 0.001 corresponds to the size of a sensor nodes sensing area. The results give evidence that existing system

provides low-quality location monitoring services for the range query with a small query region, and better quality services for larger query regions. This is an important feature to protect personal location privacy, because providing the accurate number of objects in a small area could reveal individual location information; therefore, an adversary cannot use existing system output to track the monitored objects with any fidelity. The definition of a small query region is relative to the required anonymity level k. For example, we want to provide low-quality services, such that the query error is at least 0.2, for small query regions. For the resource-aware algorithm, Fig. 8a shows that when k = 10, a query region is said to be small if its query region size is not larger than 0.002 (it is about two sensor nodes sensing area). However, when k = 30, a query region is only considered as small if its query region size is not larger than 0.016 (it is about 16 sensor nodes sensing area). For the quality-aware algorithm, Fig. 8b shows that when k = 10, a query region is said to be small if its

query region size is not larger than 0.002, while when k = 30, a query region is only considered as small if its query region size is not larger than 0.004. The results also show that the quality-aware

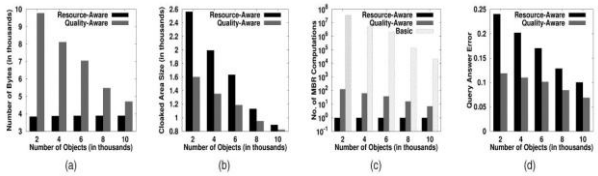
algorithm always performs better than the resource-aware algorithm.



Fig

4. Effect of the Number of Objects

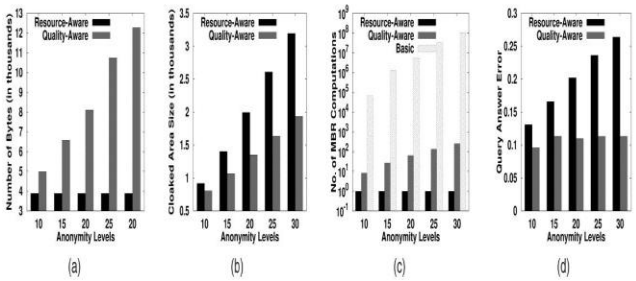
Fig. 4 depicts the performance of existing system with respect to increasing the number of objects from 2,000 to 10,000. Fig. 9a shows that when the number of objects increases, the communication cost of the resource-aware algorithm is only slightly affected, but the quality-aware algorithm significantly reduces the communication cost. The broadcast step of the resource-aware algorithm effectively allows each sensor node to find an adequate number of objects to blur its sensing area. When there are more objects, the sensor node finds smaller cloaked areas that satisfy the kanonymity privacy requirement, as given in Fig. 4b. Thus, the required search space of a minimal cloaked area computed by the quality aware algorithm becomes smaller; hence, the communication cost of gathering the information of the peers in such a smaller required search space reduces. Likewise, since there are less peers in the smaller required search space as the number of objects increases, finding the minimal cloaked area incurs less MBR computation . Since existing algorithms generate smaller cloaked areas when there are more users, the spatial histogram can gather more accurate aggregate locations to estimate the object distribution; therefore, the query answer error reduces . The result also shows that the quality-aware algorithm always provides better quality services than the resource-aware algorithm.



Fig

5. Effect of Privacy Requirements

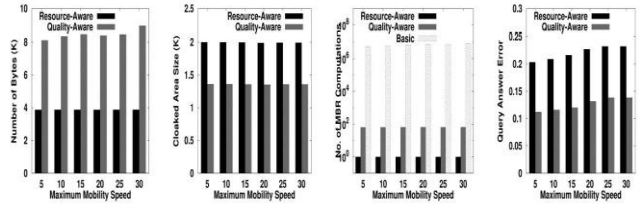
Fig.5 depicts the performance of existing system with respect to varying the required anonymity level k from 10 to 30. When the k-anonymity privacy requirement gets stricter, the sensor nodes have to enlist more peers for help to blur their sensing areas; therefore, the communication cost of existing algorithms increases (Fig5a). To satisfy the stricter anonymity levels, existing algorithms generate larger cloaked areas, as depicted in Fig. 5. For the quality-aware algorithm, since there are more peers in the required search space when the input (resource-aware) cloaked area gets larger, the computational cost of computing the minimal cloaked area by the quality-aware algorithm and the basic approach gets worse. However, the quality-aware algorithm reduces the computational cost of the basic approach by at least for existing orders of magnitude. Larger cloaked areas give more inaccurate aggregate location information to the system, so the estimation error increases as the required k-anonymity increases (Fig. 5d). The quality-aware algorithm provides much better quality location monitoring services than the resource-aware algorithm, when the required anonymity level gets stricter.



Fig

Effect of Mobility Speeds

Fig. 7 gives the performance of existing system with respect to increasing the maximum object mobility speed from 0 to 5 and 0 to 30. The results show that increasing the object mobility speed only slightly affects the communication cost and the cloaked area size of existing algorithms, as depicted in Figs. 7a and 7b, respectively. Since the resource-aware cloaked areas are slightly affected by the mobility speed, the object mobility speed has a very small effect on the required search space computed by the quality-aware algorithm. the query accuracy of the quality-aware
algorithm is consistently better than the resource-aware algorithm.



Fig

6. CONCLUSION

In this report, we studied a privacy-preserving location monitoring system for wireless sensor networks. We studied two in-network location anonymization algorithms, namely, resource and quality-aware algorithms, that preserve personal location privacy, while enabling the system to provide location monitoring services. Both algorithms rely on the well-established k-anonymity privacy concept that requires a person is indistinguishable among k persons.

In existing system, sensor nodes execute existing location anonymization algorithms to provide k-anonymous aggregate locations, in which each aggregate location is a cloaked area A with the number of monitored objects, N, located in A, where N is greater than or equal to k, for the system. The resource-aware algorithm aims to minimize communication and computational cost, while the quality-aware algorithm aims to minimize the size of cloaked areas in order to generate more accurate aggregate locations. To provide location monitoring services based on the aggregate location information, we studied a
spatial histogram approach that analyzes the aggregate locations reported from the sensor nodes to estimate the distribution of the monitored objects. The estimated distribution is used to provide location monitoring services through answering range queries.

Current work can be extended in following directions :

1. The major work to be done is for 2D space which consist of Room , Floor and Building.
2. Research for Algorithms in 2D space
3. Propose efficient containment removing algorithms.

REFERENCES

[1] Chi-Yin Chow,Mohamed F. Mokbel and Tian He ”A Privacy-Preserving Location Monitoring System forWireless Sensor Networks,”. IEEE TRANSACTIONS ON MOBILE COMPUTING, vol 10 No. 1, 2011.

[2] Dargie, W. and Poellabauer, ”Fundamentals of wireless sensor networks: theory and practice,”. John Wiley and Sons, ISBN 978-0-470-99765-9, 2010.

[3] N.B. Priyantha, A. Chakraborty, and H. Balakrishnan, ”The Cricket Location-Support System,” Proc. ACM MobiCom, 2000.

[4] B. Son, S. Shin, J. Kim, and Y. Her, ”Implementation of the Real-Time People Counting System Using Wireless Sensor Networks,” Intl J. Multimedia and Ubiquitous Eng, Vol 2, 2007.

[5] Onesystems Technologies, ”Counting People in Buildings, http://www.onesystemstech.com.sg/index.php?option=comcontenttask = viewid = 10; "2009:

[6] Traf-Sys Inc, ”People Counting Systems, http://www.trafsys. com/products/peoplecounters/ thermal-sensor.aspx,,” 2009.

[7] M. Gruteser, G. Schelle, A. Jain, R. Han, and D. Grunwald, ”Privacy-Aware Location Sensor Networks,” Proc. Ninth Conf. Hot Topics in Operating Systems (HotOS),, 2003.

[8] Dargie, W. and Poellabauer, ”Legal and Ethical Implications of Employee Location Monitoring,”. Proc. 38th Ann. Hawaii Intl Conf. System Sciences (HICSS), 2005.

[9] Location Privacy Protection Act of 2001, ”http://www. techlawjexistingnal. com/cong107/privacy/location/s1164is.asp,”. 2010.

[10]ActiveBAT, http://www.cl.cam.ac.uk/research/dtg/attarchive/bat/,”. 2005.

[11] CRICKET INDOOR POSITIONING SYSTEM, ”http://cricket.csail.mit.edu/,”. 2007.

[12] TinyOS, ”http://www.tinyos.net/,”. 2001

Text Watermarking using Encryption

Prachi Sharma[1], Deepak Chaudhary[2]
[1]*M.Tech Scholar,IET College, Alwar, Raj, India,*
[2]*Assistant Prof. IET College Alwar, Raj, India*

Abstract

Watermarking is a very active research field with a lot of applications. Although it is a relatively new field, it has produced important algorithms for hiding messages into digital signals. This work presents a new method that combines text into the image with encryption technique for safe transmission purpose. This method is based on the combination of key with watermarking. During the insertion encryption key is applied to the text during the insertion. Then, this secret key is also useful when we extract the water mark from the embedded text.

Keywords—.water mark, bit, key, etc

1 INTRODUCTION

Watermarking describes methods and technologies that hide information, for example a number or text, in digital media, such as images, video or audio. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data. The hiding process has to be such that the modifications of the media are imperceptible. For images, this means that the modifications of the pixel values have to be invisible. Furthermore, the watermark must be either robust or fragile, depending on the application. By "robust", we mean the capability of the watermark to resist manipulations of the media, such as lossy compression (where compressing data and then decompressing it retrieves data that may well be different from the original, but is close enough to be useful in some way), scaling, and cropping, among others. In some cases, the watermark may need to be fragile. "Fragile" means that the watermark should not resist tampering, or would resist only up to a certain, predetermined extent.

The example below illustrates how digital watermarking can hide information in a totally invisible way. The original image is on the left; the watermarked image is on the right and contains the name of the author.

Digital watermarks can be largely divided into fragile watermarking and robust watermarking. Fragile watermarking is mainly used for protecting data that cannot be copied, but some problems remain to be solved such as methods for data build-in and authentication, and the types of data to be inserted for data authentication. The protection of a fragile watermark can be guaranteed by maintaining security either by the

insertion method or Data-Hiding Method using Digital Watermark in the Public Multimedia Network inserted data. Robust watermarking emphasizes the robustness of the watermark information built into the digital image. Thus, the extraction of ownership information should be possible even from intentional or unintentional image transformation and lossy compression [5, 6]. As such, robust watermarking is mainly used for the ownership protection of multimedia contents.

Figure : Original Image

Figure : Watermarked Image

2. METHODOLOGY

MATLAB stands for MATrix LABoratory and the software is built up around vectors and matrices. This makes the software particularly useful for linear algebra but MATLAB is also a great tool for solving algebraic and differential equations and for numerical integration. MATLAB has powerful graphic tools and can produce nice pictures in both 2D and 3D. It is also a programming language, and is one of the easiest programming languages for writing mathematical programs. MATLAB also has some tool boxes useful for signal processing, image processing, optimization, etc.

In the MATLAB workspace, most images are represented as two-dimensional arrays (matrices), in which each element of the matrix corresponds to a single pixel in the displayed image. For example, an image composed of 200 rows and 300 columns of different colored dots stored as a 200-by-300 matrix. Some images, such as RGB, require a three-dimensional array, where the first plane in the third dimension

represents the red pixel intensities, the second plane represents the green pixel intensities, and the third plane represents the blue pixel intensities.

This convention makes working with graphics file format images similar to working with any other type of matrix data. For example, you can select a single pixel from an image matrix using normal matrix subscripting:

I (2, 15)

THIS COMMAND RETURNS THE VALUE OF THE PIXEL AT ROW 2, COLUMN 15 OF THE IMAGE I

3.OBJECTIVES

Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song, and video) within the signal itself. It is a concept closely related to steganography, in that they both hide a message inside a digital signal. However, what separates them is their goal. Watermarking tries to hide a message related to the actual content of the digital signal, while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence.

Watermarking has been around for several centuries, in the form of watermarks found initially in plain paper and subsequently in paper bills. However, the field of digital watermarking was only developed during the last 15 years and it is now being used for many different applications. A new watermarking scheme will developed to embedded text as well as image into the original image. The proposed scheme based on bit system with encryption algorithms. And reverse process for extraction the text and image from the watermarked image is discussed, after extract the text string and image compared with original image. For quantifying the error between images, like PSNR, SNR, and CRR. And some time embedded image effected by noise and due to this quality of the image degraded but this method is applicable for distortion and extracted exact string "text" and image, and check the quality of water mark image with original watermark image.

4. WATERMARKING APPLICATIONS

The increasing amount of research on watermarking over the past decade has been largely driven by its important applications in digital copyrights management and protection. One of the first applications for watermarking was broadcast monitoring. It is often crucially important that we are able to track when a specific video is being broadcast by a TV station. This is important to advertising agencies that want to ensure that their commercials are getting the air time they paid for. Watermarking can be used for this purpose. Information used to identify individual videos could be embedded in the videos themselves using watermarking, making broadcast monitoring easier. Another very important application is owner identification. Being able to identify the owner of a specific digital work of art, such as a video or image can be quite difficult. Nevertheless, it is a very important task, especially in cases related to copyright infringement. So, instead of including copyright notices with every image or song, we could use watermarking to embed the copyright in the image or the song itself.

5. WATERMARKING PROPERTIES

Every watermarking system has some very important desirable properties. Some of these properties are often conflicting and we are often forced to accept some trade-offs between these properties depending on the application of the watermarking system. The first and perhaps most important property is effectiveness. This is the probability that the message in a watermarked image will be correctly detected. We ideally need this probability to be 1.

Another important property is the image fidelity. Watermarking is a process that alters an original image to add a message to it; therefore it inevitably affects the image's quality. We want to keep this degradation of the image's quality to a minimum, so no obvious difference in the image's fidelity can be noticed. The third property is the payload size. Every watermarked work is used to carry a message. The size of this message is often important as many systems require a relatively big payload to be embedded in a cover work. There are of course applications that only need a single bit to be embedded. The false positive rate is also very important to watermarking systems. This is the number of digital works that are identified to have a watermark embedded when in fact they have no watermark embedded. This should be kept very low for watermarking systems.

Lastly, robustness is crucial for most watermarking systems. There are many cases in which a watermarked work is altered during its lifetime, either by transmission over a lossy channel or several malicious attacks that try to remove the watermark or make it undetectable. A robust watermark should be able to withstand additive Gaussian noise, compression, printing and scanning, rotation, scaling, cropping and many other operations.

WATER MARK ALGORITHMS FOR TEXT:

1. Read the input image (im).
2. Read the text string (str).
3. Convert the input image into single column.
4. Find out the length of string.
5. Check if the image size is sufficient to accommodate the string.

6. Apply bitand function to 0 the least significant bit of each element of image.
7. Find the randpermutation using randperm.
8. Apply step 9-11 for each charter of the string (for key or without key) for each bit of each character.
9. Calculation of the index of the pixels to be modified.
10. Convert each charter into 8 bit system then Apply bitget function to acquire the j-th bit of the ith character.
11. Apply bitset function to set the pixel indicated by index.
12. Inserting a character cap (end of string).
13. For each bit of the character cap.
14. Calculating the index, Updating bits into template t_im.
15. Reconstruct the watermarked image.

6. DEWATERMARK ALGORITHMS

1. Read watermarked image and key.
2. Convert the watermarked image into single column.
3. Apply randperm function for random variables.
4. Apply loop to find the character cap.
5. Using index find out the bit position using bitget function.
6. Extract the least significant bit.
7. Change combination of bit into character using and store into bitword.
8. Display the extracted image or text.

7. COMPRESSION TOOL:

Using above proposed algorithms designed a tool in MATLAB and run on MATLAN command, interface is shown in below figure.

WATER MARK INSERTION

Click on insert the water mark and first read the input image and write the test as a string (for example karan rajawat) and apply the said water mark algorithms, results are shown in below for encryption key can be inserted but key should be remember at the time of dewater marking other we cannot extract the water marked image from the embedded image.

Text as water Mark:

Figure : Input image and text **Figure : Water marked image**

8. WATER MARK EXTRACTION

Click on extract button for extract the water mark image from the embedded image, read the embedded image (encryption key which is inserted during the insertion process) and apply the said de water mark algorithms, here inserted string show which is exact same as input string results are shown in below.

Text extraction

Figure : Watermarked image and Extracted Text

Image extraction

Figure : Input image, Watermark image and Water marked image

9. QUALITY DISTORTION

In practice, a watermarked image may be altered either on purpose or accidentally. The watermarking system should be robust enough to detect and extract the water- mark [16]. Different types of alterations or attacks can be done to degrade the image quality by adding distortions.

The distortions are limited to those factors which do not produce excessive degradations; otherwise the transformed object would be unusable. These distortions also introduce degradation on the performance of the watermark extraction algorithm [17, 18]. Methods or a combination of methods, considered unintentional are used intentionally as an attack on a watermarked image in order to render the watermark undetectable.

Compression is a common attack, as data transferred via network is often compressed using JPEG. High quality images are often converted to JPEG to reduce their size. Another method is deletion or shuffling of blocks. In images rows or columns of pixels may be deleted or shuffled without a noticeable degradation in image quality. Salt and pepper noise is another type of attack that replaces the intensity levels of some of the pixels of an image resulting in loss of information from those pixels. This is used to develop a watermarking method which minimizes the quality deterioration of the watermarked im-age by finding the optimal implementation radius. With a modified coder, our method is able to adapt to the proper-ties of an image which leads to a more robust watermark while maintaining the same influence on overall quality of a watermarked image.

10. RECOVERY OF WATERMARK FROM WATERMARKED IMAGE UNDER ATTACKS

In watermarking terminology, an attack is any processing that may impair detection of the watermark or communication of the information conveyed by the watermark. The processed watermarked data is then called attacked data. There are two kinds of watermark attacks: Non-intentional attacks, such as compression of a legally obtained, watermarked image or video file, and intentional

Attacks, such as an attempt by a multimedia pirate to destroy the embedded information and prevent tracing of

Illegal copies of watermarked digital video. The present work describes only one attack:

(1) Salt and pepper noise

In this section we have demonstrated the proposed watermarking technique after using the salt and pepper noise to corrupt the watermarked images up to 0.04 with text and 0.02 for image.

Text as a water mark

Watermarked image	Extract water mark text
 Watermarked image	Karan rajawat
 Watermarked image with salt & pepper noise density:0.01	Karan rajawat
 Watermarked image with salt& pepper noise density: 0.02	Karan rajawat

 Watermarked image with salt&pepper noise density:0.03	karan rajawat
 Watermarked image with salt& pepper: noise density:0.04	karan rajawat

Here salt&pepper noise attack to water marked image(text) and we extract the water mark text fron the affected image. Result shows that text is recover without any loss of information. With different noise density text is same for each case.

INFLUENCE OF WATERMARK PARAMETERS

In the first part of the research, we evaluate the influence of the watermark on the overall quality of an image and develop a watermarking method that takes into account the influence.
There are different approaches to image quality evaluation and they are based on objective and subjective parameters. The quality of a compressed image is evaluated by analyzing the difference between the original and the compressed one.
One of the most widely used parameters for the evaluation of image quality is the MSE. The list of Image Quality measures implemented in this package include,

1. Structural Content (SC)

$$SC = \sum_{j=1}^{M}\sum_{k=1}^{N} {x_{j,k}}^2 \Big/ \sum_{j=1}^{M}\sum_{k=1}^{N} {x'_{j,k}}^2$$

2. Mean Square Error (MSE)

$$MSE = \frac{1}{MN}\sum_{j=1}^{M}\sum_{k=1}^{N}\left(x_{j,k} - x'_{j,k}\right)$$

3. Peak Signal to Noise Ratio (PSNR in dB)

$$PSNR = 10\log\frac{(2^n-1)^2}{MSE} = 10\log\frac{255^2}{MSE}$$

4. Normalized Cross-Correlation (NCC)

$$NK = \sum_{j=1}^{M}\sum_{k=1}^{N} x_{j,k}\cdot x'_{j,k} \Big/ \sum_{j=1}^{M}\sum_{k=1}^{N} x^2_{j,}$$

5. Average Difference (AD)

$$AD = \sum_{j=1}^{M}\sum_{k=1}^{N}\left(x_{j,k} - x'_{j,k}\right)/MN$$

6. Maximum Difference (MD)

$$MD = Max\left(\left|x_{j,k} - x'_{j,k}\right|\right)$$

7. Normalized Absolute Error (NAE)

$$NAE = \sum_{j=1}^{M}\sum_{k=1}^{N}\left|x_{j,k} - x'_{j,k}\right| \Big/ \sum_{j=1}^{M}\sum_{k=1}^{N}|x_{j,k}|$$

REFERENCE

[1] Ante Poljicak, Lidija Mandic, Darko Agic, "Discrete Fourier transform–based watermarking method with an optimal implementation radius",Journal of Electronic Imaging 20(3), 033008 (Jul–Sep 2011).

[2] L. N. Hu and L. G. Jiang, “Blind Detection of LSB Wa-termarking at Low Embedding Rate in Grayscale Im-ages,” In: M. Celik, G. Sharma, E. Saber and A. Tekalp, Eds., Hierarchical Watermarking for secure Image Au-thentication with Localization, IEEE Transactions on Image Process, Vol. 11, No. 6, 2002, pp. 585-595.

[3] N. F. Johnson, Z. Duric and S. Jajodia, “Information Hiding: Steganography and Watermarking—Attacks and Countermeasures,” Kluwer Academic Press, Norwell, 2001,

[4] P. Wong, “A Watermark for Image Integrity and Owner- ship Verification,” Image Processing, Image Quality, Image Capture Systems Conference, Portland, May 1998, pp. 374-379.

[5] W. Puech and j.m. rodrigues, "a new crypto-watermarking method for medical images safe transfer".

[6] Jung-Hee Seo*, and Hung-Bog Park,"Data-Hiding Method using Digital Watermark in the Public Multimedia Network",International Journal of Information Processing Systems, Vol.2, No.2, June 2006.

[7] Siddhart Manay, Byung-Woo Hong, Anthony J. Yezzi, and Stefano Soatto Integral invariant signatures, In Proceedings of ECCV 2004, number LNCS 3024, pages 87-99. Springer, 2004.

[8] Helmut Pottmann, Qixing Huang, Yongliang Yang, and Stefan KAolpl. Integral invariants for robust geometry processing, Technical report, Geometry Preprint Series, Vienna Univ. of Technology, 2005.

[9] Uccheddu F, Corsini M, Barni M. Wavelet-based blind watermarking of 3D models, Proceedings of the 2004 Multimedia and Security Workshop, Magdeburg, 143-154, 2004.

[10] Ohbuchi R, Mukaiyama A, Takahashi S. A frequency-domain approach to watermarking 3D shapes, Proceedings of Eurographics’02, Saarbrucken, 373-382, 2002.

[11]Tanmoy Kanti Das and Subhamoy Maitra “Analysis of the "Wavelet Tree Quantization" watermarking strategy and a modified robust scheme” Multimedia Syst. Vol. 12 N. 2, PP.151-163, 2006.

[12] D. S. Taubman and M. W. Marcellin, JPEG2000 – Image Compression Fundamentals, Standards and Practice, Kluwer Academic Publishers, pp.6, 2001.

[13] Ozer H., Sankur B., and Memon N., “An SVDBased Audio Watermarking Technique,” in Proceedings of the Multimedia and Security Workshop, New York, pp. 51-56, 2005.

[14] Kim H. and Choi Y., “A Novel Echo-hiding Scheme with backward and Forward Kernels,” IEEE Transactions on Circuits and Systems for Video Technology; vol. 13, no. 8, pp. 885-889, 2003.

[15] C.-H. Huang and J.-L.Wu, “Attacking visible watermarking schemes,” IEEE Trans. Multimedia, vol. 6, no. 1, pp. 16–30, Feb. 2004.

[16] R. Bangaleea and H.C.S. Rughoopth, “Performance improvement of spread Spectrum Spatial Domain Watermarking Scheme Through Diversity and Attack Characterization”, in IEEE conference Africon , pp 293-298 ,2002.

[17] Alper Koz, A. Aydin Alatan, “Oblivious Spatio-Temporal Watermarking of Digital Video by Exploiting the Human Visual System” , IEEE transactions on circuits and systems for video technology, Volume:18, Number:3, page: 326-337, March 2008.

[18] Liang Fan, Fang Yanmei, “A DWT-Based Video Watermarking Algorithm Applying DS-CDMA”, IEEE Region 10 Conference TENCON 2006, 14-17 November 2006.

[19] F. Bartolini, A. Tefas, M. Barni, and I. Pitas, \Image authentication techniques for surveillance applications," Proceedings of the IEEE, vol. 89, no. 10, pp. 1403{ 1418, 2001.

[20] M. Barni, F. Bartolini, A. Manetti, and A. Piva, \A data hiding approach for correcting errors in h.263 video transmitted over a noisy channel," in Proceedings of MMSP01, 2001 IEEE Workshop on Multimedia Signal Processing, October 3-5 2001, pp. 65-70.

[21] I. Cox, J. Kilian, F. Leighton, and T. Shamoon, \Secure spread spectrum wa- termarking for multimedia," IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687,1997.

[22] chaw- seng Woo," digital image watermarking methods for copyight protection and authenction", May 2007.

[23] M. Cancellaro, F. Battisti, M.Carli, G. Boato, “A joint Digital waterMarking and encryption method”,

[24] Melinos Averkiou "Digital Watermarking".

[25] Koushik Pal1, Goutam Ghosh, Mahua Bhattacharya2,Reversible Digital Image Watermarking Scheme Using Bit Replacement and Majority Algorithm Technique, Journal of Intelligent Learning Systems and Applications, 2012, 4, 199-206 doi:10.4236/jilsa.2012.43020 Published Online August 2012

ESTD. 1998

IET

GROUP OF INSTITUTIONS

Institute of Engineering & Technology

Alwar Institute of Engineering & Technology

Alwar Pharmacy College Alwar

Yuvraj Pratap Singh Memorial Homoeopathic Medical College , Hospital & Research Centre

www.ypsmhomoeocollege.com

Estd. 1978

SunRise University

Alwar (Raj.) | www.sunriseuniversity.in

Courses Offered

POLYTECHNIC DIPLOMA		BCA	MCA
B.TECH	M.TECH	DCA	PGDCA
D.Pharma	BBA	B.Com	M.Com
B.Pharma	MBA	LL.B.	LL.M.
M.Pharma	B.Sc.	M.Sc.	B.A.	M.A.	Ph.D.