Secure and Optimized Data Sharing Model Group in Healthcare Cloud Environment

Uma Hombal, Dayananda R.B.

Abstract-The cloud computing provides convenient on-demand access of the data. Sharing of data in the cloud computing will enable several users to easily handle the data that is being shared. The medical-field finds more advantages by the cloud-computing technology as the data can be accessed anywhere and anytime by the patients as well as this data can be shared with other medical-practitioners. This alarms for the security issues as the huge amount of sensitive data is being shared. The data must not be available to malicious-attackers. In this paper, we propose the block-design based key agreement protocol in order to share the data securely and the design provides fault-detection and fault-tolerance. The group-data model PSM is given with the block-based design, which decides how the sharing of the data is done by grouping and giving positions to users in particular blocks and the column. The $(np, i+1, 1)$ design is proposed in our paper, which gives the technique for positioning of the users. The encryption and decryption of data is done and their times cost according to file size is found. The comparison of the time-cost for our model and existing models is compared with respect to different number of simulations.

Keywords: Cloud-computing, data-sharing, block-based design, group-key

I. INTRODUCTION

Health-care requires continuous innovations in all the fields in a systematic way in order to provide high quality services. Technology of Information is rapidly and vastly used in healthcare with the motivation of to enhancing and improvising the medical services for cost reduction. Modern health-care innovations rely on information system in all aspects. The application of information-technology in health-care has got its importance in all the countries [1]. Most of the services that are provided are being outsourced to the cloud servers. The cloud storage plays a very important role in the applications like the medical files transferring etc. The majority of data being outsourced will be the health-care data, which will include the personal health record, Electronic health record and related documents. The patients are sent to various tests which results in high exchange of data between different departments of medical units. But this must be done in a secure manner. Many researches have been done to protect the data that is being shared between different departments of these medical units and to identify the risks in sharing of this data [2] [3] [4].

The technology used which helps in this data-exchange is cloud computing. Cloud computing is said to be a model that enable on demand service. The resources can be dynamically increased which implies lot of medical data can be stored and this data can be used and can be accessed anywhere and anytime by the patients or the doctors as well as share the information among them.

Revised Manuscript Received on November 08, 2019.
    Uma Hombal, Assistant Prof, Dept. of computer science and technology KLE Dr. MSSCET, Belagavi.
    Dr. Dayananda R.B., Professor, KSIT, Bangalore

This alarms for the security and privacy issues as large amount of sensitive data will be shared. The patients' data must not be accessible to malicious attackers. The compromise in this data will be a threat to both the patient and the organization with whom the patient exchanges the data. Methods are taken to provide this security against the attacks [5]

Considering this application of information technology in health-care, the personal health record being outsourced to the servers has gotten numerous data-breaches related to cloud servers which includes the malicious attacks. Patients are unable to have any physical control over their own health-record. These sensitive data are not under the control of the control of these data-owners. So there requires an encryption mechanism to protect these records before out-sourcing is done. Here the owner must decide which user will get access to which data in this record. The decryption mechanism must be such that only those with the decryption ley must be able to decrypt and obtain the data [6] [7]. This implies that the authoritative-users get the access to the data that is being shared outsourced to the cloud.

In this paper we concentrate the sharing of data to multiple users. Here the multiple users will form a group and thereby exchange the data. Here the block-based design key-agreement way is used to design the block-based design structure which can support multiple-participants. This design helps all the data holders to share their data with the higher security as well as a much more efficient manner. This presents the group data-sharing model that supports sharing of this health-care data in a group manner. This DS(data sharing) model in group provides the definition of block based design which is symmetric which determines the way communication among the groups take place. It brings the concept of group-key that the multiple participants generate to share data in a secure manner. The group members make key-agreement to derive the common group-key. This key is being generated by the users themselves. Due to this, any sorts of attacks to the key is avoided and thereby the attack on the data is avoidable. The fault-detection and fault-tolerance is provided by this design. This ensures the group-key is being generated without failure. The fault-detection is done. In this, it can identify the volunteer who can replace the malicious-attacker. This enables to avoid different key-attacks which once again makes data sharing safe. In this, the CCSTPV i.e. the cloud-security service third-party-verifier is used. This is useful in providing the key-updates. It helps the user, to encrypt the file by using the key provided by the CCSTPV and thereby outsource the data to cloud, this encryption makes the data secure for against any middle-attacks.

This paper has organized in subsequent sections that are as follows, section- 2 discuss the Literature survey, in section 3 we described proposed model, section-4 we provide the result-analysis, section-5 gives the conclusion of our paper.

Multi-tier Framework for Optimizing Pairwise Key Predistribution in Sensory Applications

Vaneeta M, S. Swapna Kumar

Abstract: *Security has been always a prominent concern in Wireless Sensor Network (WSN) irrespective of the evolution of various scientific approaches that mainly mechanizes key management approaches to secure the communication system among the resource constraints sensors. Out of various key management approaches, pairwise key is one effective approach to ensure cost effective key management scheme; however, review of existing approaches shows that they still are characterized by various issues connected to optimized performance. Adopting analytical research methodology, the proposed system implements an optimized multi-tier framework for resisting key-based threats and it targets to introduce a lightweight pair wise predistribution of keys by joint integration of enhanced public key encryption and digital signature. The study outcome shows that proposed system offer a better security performance in contrast to existing pair wise predistribution of keys.*

Keywords: *Pairwise keys, predistribution, Key agreement, Security, Attacks.*

I. INTRODUCTION

The adoption of the Wireless Sensor Network (WSN) has been prominently increasing owing to its cost effective remote monitoring capabilities [1],[2]. The sensors follow various clustering schemes in order to carry out data aggregation process [3],[4]. In such communication scheme, usually the members nodes forward the physically sensed data to their assigned cluster head which is then forwarded to either sink (using single hop) or to different cluster head (using multihop). Although, WSN is completely backed up by a stable topology as well as infrastructure, but there are always good possibilities of faults among the operations being carried out by the resource constrained sensor. There are various possibilities of intrusion in WSN both in the form of internal or external attack. There are various studies that have been discussed for addressing key agreement issue with respect to self-enforcing approach, trusted-server approach, and key predistribution approach [5],[6]. Out of all these, key predistribution scheme is found to be more used in existing system that distributes the information of secret keys is carried out before the sensors are actually deployed in the simulation. The decision of the keys can be well defined in advanced if the neighborhood information exists, which is

Vaneeta M∗, Department of Computer Science & Engineering, K.S Institute of Technology, Affiliated to VTU, Belagavi, India
S. Swapna Kumar, Department of Electronics and Communication Engineering, Vidya Academy of Science and Technology, APJ Abdul Kalam University, Thrissur, India

quite impractical as majority of the deployment strategy of the sensors are actually randomized and not on predefined basis. At present, there are various predistribution schemes in WSN that doesn't use such dependency of apriori information of the deployment of sensors. The better form of the solution will be to allow the complete set of the sensors to use a secret key that can be considered as master key. In order to achieve a better form of key-agreement, it is now feasible for different sensors to utilize this master secret key and thereby get the pairwise secret key [7]. However, such approaches are found to reduce the resiliency of the WSN performance that is not anticipated. It will mean that upon event of a compromisation of even a single sensor than the complete network will be rendered vulnerable.

Existing mechanism from the literatures recommends reposting such master key over certain form of hardware that is free from any form of physical damage or any security risk [8],[9]. It will mean that hardware-based approach is claimed to offer protection towards such master key; however it is not completely feasible as it will maximize the consumption of resources as well as cost associated with each sensor. At the same time, there is no evidence till date that hardware based security approaches are always safe as there is the possibility to break-in. There are certain other forms of the predistribution scheme of the secret keys in WSN that allows the sensors to carry a specific number of secret keys in the form of pairwise and this information is accessible only for that specific sensor node while the another specific sensor node in the form of source and destination respectively. It is claimed that such security policies are potentially strong as it is not feasible for the adversary node to influence the security strength of other sensors. Unfortunately, such approaches are not considered as practical approaches as they cannot be supported by sensors with restricted memory.

Another significant problem is that it is not feasible for adding new sensors as there is no new secret key to be allocated by the existing deployed sensors. Therefore, the proposed system discusses about a novel approach of pairwise key distribution scheme where applicability of the different test environment is valid. The idea is to ensure multi-tier framework by including a superior authentication scheme using enhanced public key encryption and digital signature. The prime agenda of the work is also to resist various forms of malicious attacks of dynamic order. The organization of the paper is as follows: Section "A" discusses about the existing literatures where different techniques are discussed for detection schemes used in power transmission lines followed by discussion of research problems in Section

Integrated System for Classification of Pulmonary Nodules on CT Images

Vijayalaxmi Mekali, Girijamma H. A

Abstract: Mortality rate of lung cancer is increasing very day all over the world. Early stage lung nodules detection and proper treatment is solution to reduce the deaths due to lung cancer. In this research work proposed integrated CADe/CADx system segments and classifies lung nodules into benign or malignant. CADe phase segments Well Circumscribed Nodules (WCN), Juxta Vascular Nodules (JVN) and Juxta Pleural Nodules (JPN) of different size in diameter. This part uses algorithms proposed in our previous WCN, JVN and JPN lung nodules segmentation work. CADx performance classification of segmented WCNs, JVNs and JPNs nodules into benign or malignant. In first part of CADx system hybrid features of segmented lung nodules are extracted and features dimension vector is reduced with Linear Discrimination Analysis. Finally, Probabilistic Neural Network uses reduced hybrid features of segmented nodules to classify segmented nodules as benign or malignant. Proposed integrated system achieved high classification accuracy of 94.85 for WCNs, 97.65 for JVNs and 97.96 for JPNs of different size in diameter (nodules diameter< 10mm, nodules diameter >10mm and < 30mm, nodules diameter >30mm and <70mm). For small nodules achieved classification performance values are, accuracy of 94.85, sensitivity of 90 and specificity of 95.85. And nodules of size 10mm to 30mm obtained accuracy, sensitivity and specificity are 97.85, 97.65 and 94.15 respectively.

Keywords : Computer Aided Detection/Diagnosis, Lung nodules, Low Dose Computed Tomography, PNN.

I. INTRODUCTION

Lung cancer is most dangerous disease with high death rate. According to 2018 lung cancer survey by World Health Organization (WHO), lung cancer new cases have risen to 2.09 million and 1.76 million deaths all over the world. Early stage detection of lung cancer is one possible and acceptable solution to reduce the death rate [17]. Lung cancer is complex disease which can be classified into different type according its site of origin, cells size, and attachment of external structures, malignancy rate and solidity. Well Circumscribed Nodules (WCN) are round or oval shaped lung nodules appears in center of lung area without any additional tissues attachment. Juxta Vascular Nodules (JVN) are attached with blood vessels and Juxta Pleural Nodules (JPN) are attached with lung pleural. At next level WCNs, JVNs and JPNs are classified into solid, part-solid and non-solid nodules. Based on severity, lung nodules are either benign or malignant.

Small nodules without cancerous cells are known as benign nodules. Moderate or large size nodules with cancerous cells are known as malignant (have potential to spread to other sites) [18]. Malignancy of malignant lung nodules indicates potential of these nodules to extent to lymph nodes, or another lung lobe or other organs like breast, brain, prostate etc. Farthest speared of malignant nodules indicates higher malignancy. Table I provides characteristics of benign and malignant nodules.

A. Low Dose Computed Tomography (LDCT) and Computer Aided Detection/Diagnosis (CADe/x) system for lung cancer

Among all the imaging modalities LDCT is GOLD STANDARD for detection of lung cancer [17]. As LDCT generates multiple CT images (slices) in one scan, interpretation of such huge number of slices by radiologist to extract the information of existence nodules is challenging task. Thus, now a days cancer detection/diagnosis medical routines uses CADe/x system to get precise information about nodules. CADe system assist the radiologist in detection of nodules and benign or malignant nodules classification is done by CADx system and it thus helps the radiologist in treatment plan. Fig. 1 is CT lung image showing different anatomical structures of lung and red circle shows the presence of lung nodule.

Fig. 1.Lung CT image with different parts and lung nodule.

Table-I: Characteristics of benign and malignant nodules

Characteristics	Benign	Malignant
Shape	Round or Oval	Irregular
Boundary Smoothness	Smooth	Irregular
Size	Less than 3cm in diameter	Greater than 3cm in diameter
Indication of cancer	Non-cancerous	Cancerous
Malignancy	No or very poor	High

Revised Manuscript Received on November 15, 2019

Vijayalaxmi Mekali, Department of Computer Science and Engineering, Kammavari Sangham Institute of Technology, Visvesvaraya Technological University, Bangalore, India. Email: duruth.viju@gmail.com

Dr. Girijamma H. A, Professor, Department of Computer Science and Engineering, R. N. S Institute of Technology, Visvesvaraya Technological University, Bangalore, India.. Email: girijakasal@gmail.com

Retrieval Number: D4414118419/2019©BEIESP
DOI:10.35940/ijrte.D4414.118419

10893

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Novel CADe/CADx System for Lung Nodules Segmentation and Classification on Computed Tomography Images

Vijayalaxmi Mekali, Girijamma H. A

Abstract: *Detection and classification of different types lung nodules poses major challenges in medical diagnosis routine. Classification of segmented nodules based on extracted hybrid features of segmented nodules have shown remarkable performance. Recently deep features alone and also with combination of hybrid features have improved nodules classification. In this research work new CADe/CADx system is proposed for detection and classification of Well Circumscribed Nodules, Juxta Vascular Nodules and Juxta Pleural Nodules. In nodules detection part, algorithms proposed in our previous work were used. Classifiers decision fusion based new nodules classification system is proposed. Four set of hybrid features and deep features using Convolution Neural Network are considered from segmented nodules. Hybrid features set consist of twenty four shape features, six GLCM features in four direction with a distance of two, six First Order Statistic features and twelve energy features. Five individually trained Probabilistic Neural Networks by all five set features separately used in nodule classification. In classification process all five classifiers decisions are fused at 2-level, 3-level, 4-level and 5-level. The proposed system achieved highest performance with 5-level fusion compared with other level fusions. System was evaluated on CT images of LIDC database with consideration of 2669 lung nodules of malignancy rate 1 to 5. Based on malignancy rate 2669 nodules are grouped as dataset 1 and dataset 2 with nodules of malignancy rate 1, 2, 3 and 3, 4,5 respectively. The 5-level decision fusion achieved highest accuracy of 95.72, sensitivity of 95.52, specificity of 95.79 and Area Under Curve of 96.21 for dataset 1 and accuracy of 92.54, sensitivity of 90.48, specificity of 94.63 and Area Under Curve of 92.69 for dataset 2.*

Keywords: **Computed Tomography, Computer Aided Detection/Diagnosis, Convolution Neural Network, Lung cancer and Lung Nodule Classification.**

I. INTRODUCTION

All over the globe mortality rate of lung cancer is very high as compared with other types of cancers such as prostate, brain, breast, cervical cancer. According to World Lung Cancer Day 2019 facts and figure, lung cancer new cases have risen to 2.09 million and 1.76 million deaths all over the world. Early stage detection and classification of lung cancer is acceptable solution to reduce the mortality rate. Lung cancer is heterogeneous disease as it appears at different

locations in lungs attached with different types of external structures with different calcification rate. Lung cancer can be classified into different type according its site of origin, cells size, and attachment of external structures, malignancy rate and solidity. Well Circumscribed Nodule (WCN) is round or oval shaped lung nodules appears in center of lung area without any additional tissues attachment. Juxta Vascular Nodule (JVN) is attached with blood vessels and Juxta Pleural Nodule (JPN) attached with lung pleural as shown in Fig. 1. At next level WCNs, JVNs and JPNs are classified into solid, part-solid and non-solid nodules. Based on severity lung nodules are either benign or malignant. Small nodules without cancerous cells are known as benign nodules. Moderate or large size nodules with cancerous cells are known as malignant (have potential to spread to other sites). Malignancy of malignant lung nodules indicates potential of these nodules to extent to lymph nodes, or to another lung lobe or to other organs like breast, brain, prostate etc. Farthest speared of malignant nodules indicates higher malignancy. Table I shows the characteristics of benign and malignant nodules.

A. Low Dose Computed Tomography (LDCT) and Computer Aided Detection/Diagnosis (CADe/x) system for lung cancer

Medical modalities like X-ray, Computed Tomography (CT), Magnetic Resonance Imaging (MRI), Positron Emission Tomography (PET) and Diffusion Weighted-MRI (DW-MRI) have been playing major role in detection of lung cancer. Among all the medical modalities Low Dose CT (LDCT) is GOLD STANDARD for detection of lung cancer. LDCT generates huge number of images (slices) in one single scans. It is tedious task for radiologist to interpret all the slices to draw useful information about existing nodules. To reduce the burden of radiologist and for accurate detection of lung cancer nodules, medical routines uses Computer Aided Detection/Diagnosis (CADe/x) system to detect and draw precise information about nodules. Benign or malignant nodules classification is done by CADx system and thus it helps the radiologist in treatment plan.

B. Role of Image processing techniques and classifier in lung cancer diagnosis

Image processing techniques such as different types of thresholding methods, Region Growing (RG) method, clustering algorithms, morphological operations, edge

Taylor & Francis
Taylor & Francis Group

Shop floor to cloud connect for live monitoring the production data of CNC machines

Prathima B A, Sudha P N & Suresh P M

Full Length Article

Power optimization in MANET using topology management

B. Devika *, P.N. Sudha

Kammavari Sangham Institute of Technology, India

ARTICLE INFO

ABSTRACT

Mobile ad-hoc network (MANET) is a wireless ad hoc network, which is quickly deployable and functions without any infrastructure. This work proposes a hybrid optimization algorithm, named Chronological-Earth Worm optimization Algorithm (C-EWA), for performing effective clustering and adjusts power and energy parameters using topology management. In this paper, initially a graph that is equivalent to the network is constructed, and then, clustering of the graph is performed using the proposed C-EWA to generate an optimal cluster head. C-EWA is developed by the integration of chronological theory in EWA, with the use of the objective function. Here, the objective function considers several factors that involve power, connectivity, mobility, link lifetime, and distance. After choosing appropriate clusters, each of the nodes that belong to the cluster constructs a Gabriel graph within the corresponding cluster. Once the Gabriel graph is constructed, each node updates the list of neighbor and maintains the graph connectivity and adjusts the power of transmission based on the connectivity. The performance of the proposed method shows superior performance in terms of remaining battery power, mobility, throughput, delay and connectivity with values of 21.960 J, 0.729, 0.713, 0.295, and 5.256, respectively.
© 2019 Karabuk University. Publishing services by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

1. Introduction

Mobile Ad-hoc Network (MANET) is an autonomous wireless ad hoc network that contains mobile nodes, which initiate transmission without considering base stations [1]. Networking is essential for the strategic networks, which are not depended on other infrastructures that involve disaster relief organizations and military [2]. Several challenges related to network protocols are presented in MANET [3]. The protocols should offer distributed solutions whenever the centralized control and the access points are absent. The node mobility is inessential as compared to routing protocols [4], which can track the topology of the network [5]. The surplus of routing protocols deployed for MANETs perform certain tasks for data transmission. The changing topologies, network division, bandwidth, larger error rates, interference, power constraints, and collision are the issues in the network control for designing larger level protocols that involve routing and executing applications using the Quality of service (QoS) [6].

The MANET is adapted in several applications that range from the battlefield to the user's living room. Due to the limited battery energy of mobile nodes, how to prolong the lifetime of nodes and network becomes the key challenge in MANET, and it has received

more and more attentions. The traditional methods employed for conserving energy are the spotlights on controlling transmission power and the dynamic turning of active nodes in the network. The reduction of energy utilization is controlled by transmission power, which subsequently results in effective data transmission and prolonging network lifetime [7]. Power plays a vital role in MANET [8,9] and requires fewer infrastructures and communication networks. The routing becomes challenging due to varying topologies produced by the movement of the node, and thus, the routing is a center of attraction among researchers. The existing routing protocols, like Ad hoc On-Demand Distance Vector (AODV) [10], Temporally Ordered Routing Algorithm (TORA), and Dynamic Source Routing (DSR), do not fulfill the requirements of real time applications. The application requires the communication network to provide a guarantee regarding QoS parameters. The prolonged battery life is important due to the mobile nodes. The power received is an important parameter for initiating the communication in MANET [11].

The MANET nodes move freely from one place to another in a random manner. The topology of the network is changed unpredictably and rapidly. The nodes inside the transmission range can directly exchange information with each other. The nodes that reside outside the transmission range should communicate indirectly by adapting the multi-hop routing protocol. Each node is responsible for the route discovery in a dynamic manner. Despite several clustering schemes, the organization of MANET into a

* Corresponding author.
E-mail address: devikabgowda@gmail.com (B. Devika).
Peer review under responsibility of Karabuk University.

Edge Detection and Contour Based Ear Recognition Scheme

Deven Trivedi, G. H. Patel College of Engineering and Technology, Anand, India

Rohit Thanki, C. U. Shah University, Wadhwan, India

https://orcid.org/0000-0002-0645-6266

Surekha Borra, K. S. Institute of Technology, Bengaluru, India

ABSTRACT

In recent days, with the advancements in computer vision technology pattern recognition for biometric data has been the focus of many researchers. The human ear can be used to assist in the recognition of an individual. In this article, a new scheme for ear recognition is presented, based on edge features such as the helix shape and contours between the edge pixels. First, an ear image is detected from the acquired image using a snake model-based image segmentation technique, and then histogram equalization is applied to form an enhanced ear image. After that, an Infinite Symmetric Exponential Filter (ISEF) edge is applied to the image, the contouring of edges is calculated, and then the contour values of pixels are extracted as ear features. Finally, the ear matching is performed between query ear features and enrolled ear features. Based on the matching score, the decision about individual authentication is performed. The experimental results showed that this proposed scheme performs better than existing schemes in the literature.

KEYWORDS

Biometric, Canny, Contour, Ear, Edge, Shen-Castan

1. INTRODUCTION

Nowadays, an individual is recognized based on his/her biometric characteristics in many places like offices, institute, airports, etc. These biometric characteristics are divided into two types: physical and behavioral (Jain and Kumar, 2012; Jain and Nandakumar, 2012). The examples of physical characteristics of an individual are fingerprint, face, iris, palm print and ear. The examples of behavioral characteristics of an individual are speech, signature, and gait. The systems based on biometrics recognize an individual automatically using various computer vision and pattern recognition algorithms (Jain and Kumar, 2012; Jain and Nandakumar, 2012). The biometric systems are used mainly for two operations: verification and authentication. In these operations, the query biometric image is compared and matched with its closest image in the database. While the query image is compared with all the database images in case of authentication, it is compared with its enrolled image in case of verification.

Cost-Effective Spectrum Utilization for Futuristic Cognitive Radio based Services

Chanda V. Reddy

Abstract: The proliferation of various mobile users in the context of advanced wireless technologies, spectrum scarcity arises as a crucial problem. The notion of cognitive radio (CR) principle offers cost-effective spectrum reusability with intelligent mode of transmission model. It basically enables a radio-driven technology to utilize dynamic spectrum accessing to meet the quality-of-services (QoS) requirements by satisfying enormous communication and connectivity demands. To alleviate the spectrum scarcity problem the study proposes a novel analytical solution of spectrum allocation considering a simplified evolutionary learning model. The prime target of the formulated concept is to detects the spectrum holes effectively for reusability and the possibility of identification has be maximized for best possible spectrum allocation to the radios. And on the other hand also the occurrence of false positive identification has to be minimized. The outcome obtained after performing the simulation shows promising aspects in the context of effective spectrum. allocation for higher priority user with better throughput performance.

Keywords: Cognitive Radio, Spectrum Allocation, multi-objective optimization, Throughput performance

I. INTRODUCTION

In the recent scenario researchers from IEEE and many other communication societies are more concerned towards improving the communication paradigm in the context of 5G wireless technologies. The underlying principle of cognitive radio (CR) technology opens up a new opportunity for effective spectrum utilization and also aroused significant attention for its wider prospects [1] [2]. CR has been introduced to tackle the issue connected with the constraints of bandwidth availability of conventional wireless communication standards which is tightly licensed and restricted by the Government policies. Thereby, it can be seen that mobile devise are restricted to utilize a certain value of frequency and hence a bottle-neck scenario arises in reality due to limited bandwidth where the number of mobile users are tremendously increasing. Thereby maintain quality of service aspects (QoS) with effective spectrum utilization has become crucial. CR technology can easily handle this issue of spectral scarcity by meeting the growing demand of mobile user requirements and also has become a reliable solution to solve the spectral congestion problem in the modern wireless communication [3][4]. CR is utilized as an extended technology component of software defined radio (SDR) and also incorporates an intelligent system of sensing and channel management functionality. There exist various time-critical applications of CR such as into public safety networks,

Revised Manuscript Received on February 06, 2020.
* Correspondence Author

Dr. Chanda V.Reddy*, Professor and Head, Department of TCE, Kammavari Sangham Institute of Technology, Bangalore, India, Email: chandavreddy@ksit.edu.in

disaster relief and emergency networks etc. and it is highly agile for advanced intelligent communication systems considering its autonomous mode of selection of operating parameters [5][6]. The figure 1 presents and overview of the advanced paradigm in CR based radio communications.
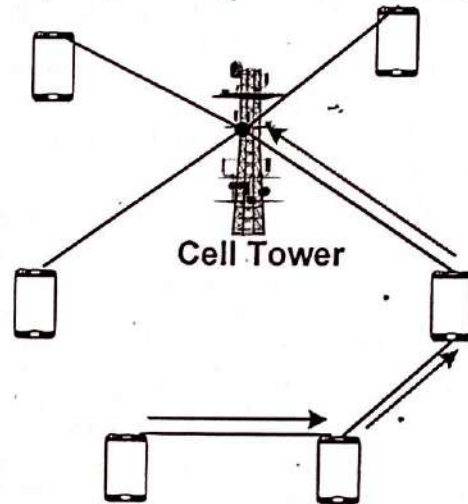

Fig 1 Radio communication in CR

Fig.1 shows that how the CR enabled communication facilitates mobile devices to communicate with each other so that communication between a mobile client and cell-tower can be established with higher throughput efficiency [7][8]. This research study addresses the spectrum allocation problem in the modern wireless communication technology and aims to formulate an energy efficient optimized transmission model based on CR to attain better end-to-end throughput performance. The system modeling of CR is designed with an objective to perform intelligent resource scheduling in variable traffic conditions in the context of advanced cellular networking operations. For this purpose the methodology aims to maximize the spectrum utilization performance considering a metaheuristics evolutionary learning model with lower complexity to attain best possible outcome. The entire manuscript is presented with respect to different sections, *section II* highlights the existing trend of research based studies on CR and outlines the gap in reality. *Section III* finally extracts the cumulative research problem which is jointly addressed in this study with problem formulation aspect.

Finally section IV highlights a comprehensive discussion on proposed analytical system design for CR assisted effective spectrum resource management.

The mathematical modeling is formulated for best possible available spectrum allocation to the SDR with higher possibility of available spectrum detection and also minimizing

☐   4010

A novel and integrated architecture for identification and cancellation of noise from GSM signal

Rekha N[1], Fathima Jabeen[2]
[1]Department of Electronics and Communication Engineering, K.S. Institute of Technology, India
[2]Islamiah Institute of Technology, India

ABSTRACT

There are multiple reasons for the evolution as well as the presence of noise over transmitted GSM signal. In spite of various approaches towards noise cancellation techniques, there are less applicable techniques for controlling noise in acoustic GSM signal. Therefore, the proposed manuscript presents an integrated modelling which performs modelling of noise identification that could significantly assist in successful noise cancellation. The proposed system uses three different approach viz. i) stochastic based approach for noise modelling, ii) analytical-based approach where allocated power acts as one of the prominent factors of noise, and iii) wavelet-based approach for effective decomposition of GSM signal for assisting better noise cancellation technique followed by better retention of signal quality. Simulated in MATLAB, the study outcome shows that it offers a cost-effective implementation, A Practical Approach for Noise identification, and Effective Noise Cancellation with Signal quality retention. The proposed system offers approximately 24% of enhancement in noise reduction as compared to any existing digital filters with 1.6 seconds faster in processing speed.

Corresponding Author:

Rekha N,
Research Scholar, Department of Electronics and Communication Engineering,
K.S. Institute of Technology, Bengaluru, India.
Email: rekhaphd2014@gmail.com

1. INTRODUCTION

Since last few years, the GSM-based wireless communication has been accounted for emerging growth in the telecom industries. The GSM was introduced as a progression of second-generation cellular technology specified with digital modulation service. At present, the development of the GSM standard has reached the level of meeting daily needs of users and enterprises by providing cost-effective voice services as well as efficient data services which can be accessed 24x7 irrespective of user's location [1]. GSM technology supports various features for its global acceptance and rich popularity [2]. Such features are like it has efficient spectrum, good voice quality service supports low-cost cellular devices, compatible with ISDN and new services and provides roaming services globally. With the evolution of GSM, there are many advances made in digital devices, such as personal digital assistants, PCs, mobile phones, wireless LANs, etc [3]. These devices are enabled with the support of cellular communication module in order to deliver on-demand services and entertainment in various fields of application such as schools, office, healthcare, transport, Industrial area, and many more [4].

In a cellular communication system, the speech and data information transmitted via a radio link communication channel where the quality of transmitted data suffers from many degradation factors such as background noise and channel interferences [5]. The 'term' noise and interference basically refers to unwanted destructive signals introduced into use-full speech and data signals. The sources of noise are varied in nature it can be generated from an environmental factor such as acoustic disturbance form traffic, blowing

Implementing and analysing FAR and FRR for face and voice recognition (multimodal) using KNN classifier

Dinesh Kumar D.S.

TJIT, Visvesvaraya Technological University, Belagavi, India and KSIT, Bangalore, India, and

P.V. Rao

TJIT, Bangalore, India and VBIT, Hyderabad, India

Abstract

Purpose – The purpose of this paper is to incorporate a multimodal biometric system, which plays a major role in improving the accuracy and reducing FAR and FRR performance metrics. Biometrics plays a major role in several areas including military applications because of robustness of the system. Speech and face data are considered as key elements that are commonly used for multimodal biometric applications, as they are simultaneously acquired from camera and microphone.

Design/methodology/approach – In this proposed work, Viola–Jones algorithm is used for face detection, and Local Binary Pattern consists of texture operators that perform thresholding operation to extract the features of face. Mel-frequency cepstral coefficients exploit the performances of voice data, and median filter is used for removing noise. KNN classifier is used for fusion of both face and voice. The proposed method produces better results in noisy environment with better accuracy. In this proposed method, from the database, 120 face and voice samples are trained and tested with simulation results using MATLAB tool that improves performance in better recognition and accuracy.

Findings – The algorithms perform better for both face and voice recognition. The outcome of this work provides better accuracy up to 98 per cent with reduced FAR of 0.5 per cent and FRR of 0.75 per cent.

Originality/value – The algorithms perform better for both face and voice recognition. The outcome of this work provides better accuracy up to 98 per cent with reduced FAR of 0.5 per cent and FRR of 0.75 per cent.

Keywords FAR, LBP, MFCC, DCT, KNN

Paper type Research paper

1. Introduction

In the modern world, biometrics is used to authenticate and identify a person. Biometrics combines the physical traits and behavioural characteristics for identity verification. It provides a suitable solution to our security needs with better accuracy. A person can be identified accurately using biometrics based on unique physical or behavioural characteristics. Multimodal biometric authentication is widely used in banking security, credit card transactions and passport verification combining different biometric traits.

1.1 Problem statement

Biometrics is widely used for authentication and identification of a person based on physiological and behavioural traits such as face, iris, palm print, signature, etc. There are several drawbacks of unimodal biometric systems such as intra-class variation, inter-class

Power-Cognizant Proactive Routing Protocol for Amending Energy in Ad-hoc Networks

B. Devika[✉] and P. N. Sudha

KSIT, Bengaluru, India
{devikabgowda, pnsudha}@gmail.com

Abstract. The execution of an Ad hoc Wireless Network is controlled by a key factor "power", as it is the essential resource of any communication system. Utilizing such power effectively and efficiently is the most important Task. Power has to be optimized according to the requirement. In an ad hoc network, nodes exchange information with each other by forming a multi-hop wireless network & sustaining connectivity in a localized fashion. Optimizing power in such a network is a significant challenge ad hoc routing protocols are power hungry as they expend a substantially large amount of battery power contained in the nodes. Hence routing in an ad hoc network is eminently power restricted. Research has been done choosing the appropriate routing protocol at the network layer and power aware protocol at MAC layer. In this paper, a proactive routing protocol has been implemented which is power aware. FSR is the routing protocol chosen and MAC 802.11 standards have been used in combination of a routing protocol to optimize power. The simulation is executed using NS-2 and the power consumption has reduced.

Keywords: Ad hoc networks · Fisheye state · Manet · Mac · Power cognizant

1 Introduction

Wireless communication is the quickly expanding & most vital technological areas in the communication field. Our lives are unimaginable without Wireless communication like TV, Radio, Mobile, Radar, GPS, Wifi, Bluetooth, RFID etc. In Latin ad hoc means "for this purpose". Ad hoc networks are group of self-organizing nodes or terminals that exchange information with each other by combining a multi-hop wireless network and sustaining connectivity in a suburbanized manner in an infrastructure less environment. Several classifications of Ad hoc networks are MANET, VANET, FANET, WSN etc. Ad hoc network operate with IEEE 802-11 standards. Initially ad hoc networks were designed for military and disaster recovery applications, due to their fast deployment feature without the existence of any infrastructure. But with rapid growth of mobile communication, MANETs are regarded as important contemplate in the future inception of system technologies [1].

Various power optimization techniques are existent in Ad hoc networks. Optimization of power is of at most importance in Ad hoc networks as their structure is autonomous and non-existence of central governing body. Various layers are affected while optimizing power in ad hoc network like physical, network & MAC layer [2].

© IAEME Publication   Scopus Indexed

A COMPARATIVE ANALYSIS OF DES AND BAES FOR MANET

Srividya R

K. S. Institute of Technology, Bangalore, Karnataka, India

Ramesh B

Department of Computer Science and Engineering,
MCE - Malnad College of Engineering, Hassan, Karnataka, India

ABSTRACT

The exponential increase in digital data exchange in Mobile Ad hoc network paves a way for authentic research in the horizon of securing data using cryptographic methods. This paper proposes a comparative analysis of existing DES and proposed Biometric Advanced Encryption Standard (BAES) cryptographic algorithm. BAES implementation includes design of robust biometric key generation algorithm that can mitigate malicious attacks by extending security definitions of existing Advanced Encryption Standard.

Key words: MANET, BAES, DES, Fingerprint, Minutiae.

1. INTRODUCTION

Mobile Ad hoc Network (MANET) is known for its self configuring and dynamic nature and its capability to exchange data between mobile nodes. Due to MANET's dynamic nature, providing secure data mobility is a challenging task. Passive or active attacks can be launched effortlessly in such networks with no centralized management and firewall. To secure the data from being permuted or eavesdropped is a confronting assignment. It is intricate to detect passive attacks like eavesdropping. Hence the outstanding schema would be to use a cryptographic method and encrypt the data before transmitting it into MANET. The past few decades have seen an exponential rise in the genre of cryptographic algorithm innovations and inventions. The study of literature illustrates ample of encryption algorithms and their applications. Here we propose and develop a cryptographic method Biometric Advanced Encryption Standard (BAES), which is a petty contribution to the sphere of cryptographic algorithms. An effort is put in, to compare BAES with Data Encryption Standard (DES) considering time and memory parameters.

☐   4266

Implementation of AES using biometric

Srividya R[1], Ramesh B[2]
[1]Department of Telecommunication Engineering, K.S. Institute of Technology, India
[2]Department of Computer Science and Engineering, Malnad College of Engineering, India

Article Info	ABSTRACT
	Mobile Adhoc network is the most advanced emerging technology in the field of wireless communication. MANETs mainly have the capacity of self-forming, self-healing, enabling peer to peer communication between the nodes, without relying on any centralized network architecture. MANETs are made applicable mainly to military applications, rescue operations and home networking. Practically, MANET could be attacked by several ways using multiple methods. Research on MANET emphasizes on data security issues, as the Adhoc network does not befit security mechanism associated with static networks. This paper focuses mainly on data security techniques incorporated in MANET. Also this paper proposes an implementation of Advanced Encryption Standard using biometric key for MANETs. AES implementation includes, the design of most robust Substitution-Box implementation which defines a nonlinear behavior and mitigates malicious attacks, with an extended security definition. The key for AES is generated using most reliable, robust and precise biometric processing. In this paper, the input message is encrypted by AES powered by secured nonlinear S-box using finger print biometric feature and is decrypted using the reverse process.

Corresponding Author:

Srividya R,
Department of Telecommunication Engineering,
K.S. Institute of Technology,
#14, Raghuvanahalli, Kanakapura main road, Bangalore-109, India.
Email: srividya.ramisetty@gmail.com

1. INTRODUCTION

MANET is a wireless Adhoc Network which is dynamic in nature. It has the capability to transmit signals in between mobile nodes. Its self-configuration property essentially deals with dynamic property of moving nodes. MANET does not have organized network infrastructure in order to establish communication, because of its agility. This imposes limitations on network infrastructure, data security, processing ability, throughput and performance of the system [1]. Data security for MANET is to be designed keeping processing power and speed into consideration. Hence the deployment environment defines an extensive security at the cost of low processing power and at high data rate. MANET has on-demand need for high level security systems incorporated in network infrastructure. The literature stream lines wide number of security systems applicable to network systems. Most popular Cryptographic system illustrated in literature is advanced encryption system (AES). AES is distinguished encryption and decryption system used widely in vital computer networking applications. Key generation used to encrypt input message is again a very important aspect in data encryption/decryption systems. Use of symmetric key and asymmetric key remarks its own merits and demerits in securing data and data mobility in MANETs.

Main motivation behind data security in context of MANET is not only to secure data at high speed, but also at reduced processing power. Hence the usage of key generation is limited to implementation of symmetric key generation. However symmetric key generation is also made complex by generating the key