Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 167 (2020) 2382–2392

Procedia Computer Science

www.elsevier.com/locate/procedia

International Conference on Computational Intelligence and Data Science (ICCIDS 2019)

Image Quality Assessment Parameters for Despeckling Filters

Rajeshwar Dass[a], Niranjan Yadav[b]

[a]*Assistant Professor, ECED, DCRUST, Murthal*

[b]*Ph.D Scholar, ECED, DCRUST, Murthal*

Abstract

Images Quality assessment shows vital role in image processing applications and is an active field of research. In medical imaging field various imaging modalities i.e. Ultrasound (US), X-ray, Computer Tomography (CT) and Magnetic Resonance Imaging (MRI) etc. are used to diagnose the disease by the doctors. In US imaging modality coherent sources are used for imaging purpose. Due to coherent sources, speckle noise inserts in US images and causes loss of information and blurring which leads to misdiagnose of the patients by the doctors. To avoid this situation, various despeckling filters are used to remove the speckle noise and their performance is analysed on the basis of subjective and objective assessment parameters. This paper summarizes the various performance evaluation parameters i.e MSE, RMSE, SNR, PSNR, AD, SI, NK, MD, LMSE, NAE, IQI, SSIM, and BETA, their significance & relevance with the example of despeckling filters i.e. LEE Sigma, Detail Preserving Anisotropic Diffusion (DPAD), Fourier Butterworth Filter (FBF), ROFTV (Rudin, Osher and Fatem) and Hybridized Mean and Wiener Filter.

Keywords: Objective & Subjective assessment parameters; LEE Sigma, Detail Preserving Anisotropic Diffusion (DPAD), Fourier Butterworth Filter (FBF), ROFTV (Rudin, Osher and Fatem) and Hybridized Mean and Wiener Filter.

1. Introduction

Ultrasound (US) imaging modality uses sound waves to produce images of the organ within the human body. Ultrasound imaging modality is non-ionized in nature and is generally used to estimate lumps or lesion in the human body, found during a predictable physical or other imaging examination[1]-[3]. Multiplicative noise named as speckle noise produces by interfering echoes of transmitting wave form, which generates from heterogeneities of the organ being cross examined [4]. It is an inherent property present in the US and it treads to minimizing the image resolution, contrast and remove or reduced the diagnosis information for this imaging modality [4]-[6]. Speckle noise inclines to reduce the quality and reliability in the US images [1]-[2]. Image processing play an important role for suppressing

1877-0509 © 2020 The Authors. Published by Elsevier B.V.

10.1016/j.procs.2020.03.291

Texture Analysis of Liver Ultrasound Images

Niranjan Yadav, Rajeshwar Dass, and Jitendra Virmani

Abstract The main goal of this work is to classify liver ultrasound images based on texture features for the early detection of liver abnormalities. A total of 60 liver ultrasound (30 benign and 30 malignant) images have been used for the analysis. A total of 302 texture features have been extracted, namely histogram, co-occurrence matrix, run-length matrix, absolute gradient, autoregression, and wavelet-based by using MaZda. In this work, most uncorrelated features are selected using principal component analysis (PCA), and three classifiers, namely (a) probabilistic-neural network (PNN), (b) K-nearest neighbors (K-NN), and (c) support vector machine (SVM) has been used to classify liver abnormities. A total of 20 statistical features have been selected using PCA and SVM yields optimal accuracy as 95%. It is observed that texture analysis using the MaZda package has been a more feasible and convenient method for analysis of abnormalities of the soft tissue.

Keywords Texture analysis · MaZda · PCA · SVM · GLCM · GLDS · GLRLM

1 Introduction

Various medical imaging modalities are widely used for characterization of soft tissue as x-ray, ultrasound, MRI, PET CT scan. Sonography has been widely used for analysis of soft tissue due to (a) low cost, (b) radiation free, (c) easy availability [1, 2]. The sonography reveals the texture of the soft tissue includes appearances, position, and structure of lesion. The texture features of an image are computed using several mathematical process by evaluation of grayscale intensity and position of pixel [3, 4]. Texture analysis provides intra-lesion heterogeneity and relationship among, the gray-level values in the image [5]. The histogram-based texture features mean, variance, skewness, and kurtosis attains uniformity, histogram as asymmetry,

N. Yadav (✉)
DCRUST Murthal, Sonipat, India

R. Dass · J. Virmani
CSIR-CSIO, Chandigarh, India

N. Marriwala et al. (eds.), *Emergent Converging Technologies and Biomedical Systems*,
Lecture Notes in Electrical Engineering 841,
https://doi.org/10.1007/978-981-16-8774-7_48

2022 International Conference on Smart and Sustainable Technologies in Energy and Power Sectors (SSTEPS)

Enhancing the Security of STOMP Protocol and Its Comparison with other Encryption Methodologies

Sarita Kumari
Department of CSE
RPS Groups of Colleges
Mahendragarh, India - 123029
saritanaveenkaliraman@gmail.com

Sangeeta Gulia
Department of CSE
Central University of Haryana
Mahendragarh, India - 123029
army.sangeeta46@gmail.com

Vikas Raman
Department of CSA
Chaudhary Ranbir Singh University
Haryana, India- 126102
vikas.raman92@gmail.com

Thirupathi J
Department of CSE
Institute of Aeronautical Engineering
Hyderabad, Telangana, India- 500043
thirupathi.j@iare.ac.in

***Abstract* - Internet is seeming to be a vital need for each and every person in today's world, by which the inter-connectivity also comes into scenario. As a result of this new innovation which is created using Internet covers the whole market. Then IoT (Internet of Things) arise and which helps to connect device and human being for various purposes. Here the gadget contains various kind of sensors and power sources, and all devices and human being can communicate each other for single or multiple tasks. Today IoT discover devices are works over the Cloud, so there is a need for security arises. Instead of which anywhere and anyone can access and misuse that information. Also the unauthorized person able to see and change the structure of architecture. In this paper we will discuss various types of message passing protocols used with IoT for transferring confidential information. Here we try to upgrade level of security while works with IoT and to build a secure end to end connectivity between devices.**

Keywords* - *Hash Message Authentication Code (HMAC), Simple Text Oriented Messaging protocol (STOMP), Internet of Things (IoT), Extensible Messaging and Presence Protocol (XMPP), Transport Layer Security (TLS),

I. INTRODUCTION

Now a day, the cyber attackers tries to enter any secured firewall and destroying the high security levels provided by the system. By this the attackers just want to make a large amount of information loss to the target organization. From the last few years, the problem related to IoT comes into scenario. Today the attackers are expert to capture the data transmission actively during communication between various devices. Attackers apply so many types of penetration attacks over the targeted device to access the network bandwidth and various resources by sending a pool of packets to the targeted machine. Once they intercept between the devices data transmission process they start try to act as client or peer and request to host at other side for their response or to change the previously existing algorithm of program. By doing this they lead existing IoT device to read wrong or false data [1].

There are many message passing protocols which are used in the domain of IoT today. One of the most important message passing protocols is STOMP [2]. STOMP protocol which is a message passing protocol can provide an interactive wire format, so that all the clients working with STOMP can communicate with message broker can messaging very easily and can interoperable into many languages and platforms [3]. STOMP messaging protocol has ability of messaging clients in any language just within a very short'period of time. Till now there is no encryption mechanism of STOMP is available. Up to today, STOPM send messages or information payloads as a simple plain text using TCP over wired medium [4]. So we can say that STOPM itself requires an end to end encryption, for passing the message payload securely between clients by focusing on vulnerability.

II. TARGATED ATTACKS ON IOT

There are so many surveys going on IoT now days. The attackers are also getting up to date to become compatible with today's message transmission domain. They try to analyze the existing encryption mechanism currently implemented and perform reverse engineering over those methods in the complex virtual IoT ecosystem. As we all know IoT has spread each and every sector like Government department, corporate sectors etc. the data security kept inside is very important [1].

A. Messaging Passing Protocols

There are various kind of messaging protocols for IoT has been introduces till now with useful features. But besides this only some of the protocols are used for IoT based message passing mechanism. All message passing protocols have different applications and security features as compared to each other. The End to End detailed clarification of encryption mechanisms are given to all the clients which are sending message to all the brokers. In some of the messaging protocols the brokers are situated in the middle IoT sensors and messaging clients. The IoT sensors generate some output values and the intermediate interface send these output values to message brokers, then after that broker creates queues to store the sensors generated values and later publishes these output values to the subscriber Clients which can compute the final results [7]. Below Fig.1. Shows the complete process of

978-1-6654-6414-7/22/$31.00 ©2022 IEEE
DOI 10.1109/SSTEPS57475.2022.00077

RabbitMQ Message broker, and communication between publisher and subscriber.

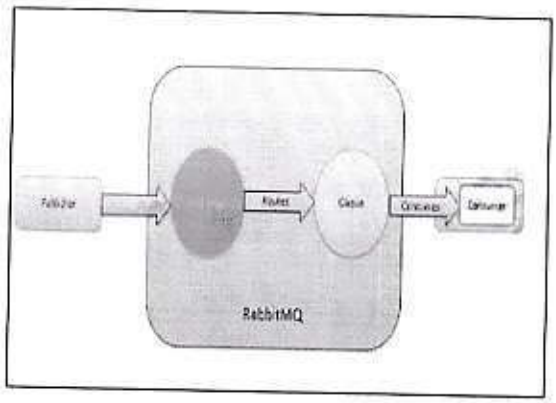

Fig. 1. Process Flow of RabbitMQ message broker

B. *DDoS Attacks*

A Denial of Service or DoS attack is an intentional attempt by its culprit to disable a functional network or all online resource, typically with an unwanted kind of activity. So for the person or group of persons who secretly plan for DoS and DDoS attacks, IoT software, hardware with the help of number of processes and devices that may be fully infected with malwares and called during bidding. The largest Attack (DDoS) in history which can nearly destroy complete Internet is the Guardian News & Media Limited reported on 2016 [5]. In this DDoS attack the malware totally control a large number of gadgets and smart devices to break their interfaces. As a result of this, a requirement of encryption to protect the message and information during transmission arise.

III. STOMP PROTOCOL

STOMP also provides an interactive and interoperable format by which all STOMP clients can be able to communicate with any other STOMP message broker and provide very easy messaging interoperability among so many languages, brokers and platforms. STOMP messaging protocol doesn't provide any specific protocol frame related to message payload security. It can use plain text or binary format for sending the produced message [3]. It can use "UTF-8" for its default encoding. Beside this it can use some other encoding also. Some external libraries also developed by developers for providing security to the STOMP protocol. All libraries are not performing well with STOMP but some provides good encryption mechanism while applying. The comparison between various kind of messaging protocols has done for analyzing that which encryption performs good during transmission. From the pool of mechanisms, some are also used with other protocols too like Login authorization security, TLS security and symmetric key encryption. But these methods have some major limitations that any can breach the data and perform a malware attack. If we work with TLS security, it only applied when verifying the medium or channel so the chances of risk are very high and overhead for this is very high as compared to the amount of data. At the end, we can apply HMAC mapping for message encryption which is more confidential and faster as compared to symmetric key encryption algorithm [8].

IV. SECURITY MECHANISM

A. *Current Methodologies*

Some other protocols for messaging used are AMQP, MQTT, XMPP and HTTP with TLS as their message security mechanism over UDP (User Datagram Protocol) or TCP (Transmission Control Protocol) from where the medium can perfectly be seen Table.1. There is a major drawback of using TLS payload encryption, in which the limitation present inside the implementation, so the intruder or attackers have the access at transport layer, drop in traffic and slower in transportation of message while using TLS for websites. According to the reference [9] in past few years, so many attacks cases made over TLS, which includes ciphers and method of operations. As an output if current used protocols TLS act as a main payload security.

TABLE I. PROTOCOL COMPARISON

Criteria	AMQP	MQTT	XMPP	STOMP
Goal	Replacement of proprietary protocols	Messaging for resource constrained devices	Instant messaging, adopted for wider use	Message oriented middleware
Format	Binary	Binary	Xml-based	Text-based
API	Divided into classes	Simple(5 operations with 2-3 packets types for each)	Different xml items with multiple types	~ 10 basic commands
Reliability	Publishes/subscriber acknowledgements	acknowledgements	Acknowledgements and resumptions	subscriber acknowledgements, transactions
Security	SASL,TLS/SSL	No built-in TLS/SSL, Header authentication	SASL,TLS/SSL	Depending on message Broker
Extensibility	Extension points	None	Extensible	Depending on message Broker

B. *Protocol Comparison*

In Table.1, we try to compare different kind of message encryption protocols which are MQTT, AMQP, XMPP and STOMP. In this message transmission process, all these protocols act as medium of transfer from publisher client to subscriber client via server. Security features will be considered for all the protocols [10].

V. EXISTING ANALYSIS

A. Algorithm Analysis

SHA1 and MD5 plays an important role in hashing cryptographic encryption for securing the web globe [11]. So the comparison between all kind of hashing algorithms such as SHA-1, SHA-2, SHA-3, MD5etc. Some hashing functions are very fast for performing encryption process. And the most effective hashing i.e. AES hashing is slower than other hashing functions. HMAC is selected from Black2, SHA3-256 and SHA3-224. And Black2 is much faster than SHA2, SHA3 in producing the digest [13].

B. Hash Message Authentication Code

Text to HMAC conversion depends upon the idea on rainbow ambush table, where an attacker hashing code can examine the basic secret key from a hashed motivator by using hash table. It is available for anybody to fix the hash table for their own requirement. HMAC algorithm can use HMAC code for its mapping to generate signatures. The attacker would not be able to generate mapping table without secret key. For every message the hashes must be identified and look through pool of keys to find out perfect match for decrypting the payload send by client [12].

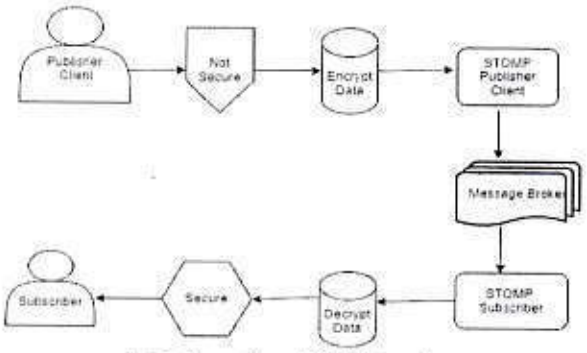

Fig. 2. Process Flow of HMAC Encryption

VI. CONCLUSION

After studying all these comparisons and analysis, it is proved that till now no researcher can have made any attempt for analyzing and research on encryption algorithm over STOMP payload message encryption. Therefore, it is proved that lot of scope is available for research contribution towards invention of effective and fast message encryption mechanism for better encryption algorithm to enhancing security during transmission of message from producer client to subscriber client [14]. So that it will be possible that attacker won't be able to breach the security through messaging layers and through the data transmission between the clients.

REFERENCES

[1] Wang, Jingyuan, et al. "TCP-FIT: An improved TCP congestion control algorithm and its performance." *2011 Proceedings IEEE INFOCOM*. IEEE, 2011.

[2] Chaudhary, Ajay, Sateesh K. Peddoju, and Kavitha Kadarla. "Study of internet-of-things messaging protocols used for exchanging data with external sources." *2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*. IEEE, 2017.

[3] Celar, Stipe, Eugen Mudnic, and Zeljko Seremet. "State-of-the-art of messaging for distributed computing systems." *International Journal Vallis Aurea* 3.2 (2017): 5-18.

[4] Fortino, Giancarlo, et al. "Towards multi-layer interoperability of heterogeneous IoT platforms: The INTER-IoT approach." *Integration, interconnection, and interoperability of IoT systems*. Springer, Cham, 2018. 199-232.

[5] Woolf, Nicky. "DDoS attack that disrupted internet was largest of its kind in history, experts say." *The Guardian* 26 (2016).

[6] Chen, Xiaofeng, Fangguo Zhang, and Kwangjo Kim. "Chameleon hashing without key exposure." *International Conference on Information Security*. Springer, Berlin, Heidelberg, 2004.

[7] Hakiri, Akram, et al. "Publish/subscribe-enabled software defined networking for efficient and scalable IoT communications." *IEEE communications magazine* 53.9 (2015): 48-54.

[8] Ovsytenko, D. *Babel Hashed Message Authentication Code (HMAC) Cryptographic Authentication*. No. rfc7298. 2014.

[9] Sheffer, Yaron, Ralph Holz, and Peter Saint-Andre. *Summarizing known attacks on transport layer security (TLS) and datagram TLS (DTLS)*. No. rfc7457. 2015.

[10] Naik, Nitin. "Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP." *2017 IEEE international systems engineering symposium (ISSE)*. IEEE, 2017.

[11] Johnsen, Frank T. "Using publish/subscribe for short-lived iot data." *2018 Federated Conference on Computer Science and Information Systems (FedCSIS)*. IEEE, 2018.

[12] Nastase, Lavinia. "Security in the internet of things: A survey on application layer protocols." *2017 21st international conference on control systems and computer science (CSCS)*. IEEE, 2017.

[13] Tiwari, Harshvardhan, and Krishna Asawa. "A secure and efficient cryptographic hash function based on NewFORK-256." *Egyptian Informatics Journal* 13.3 (2012): 199-208.

[14] Chodorek, Agnieszka. "TCP and TCP-friendly protocols." *Encyclopedia of internet technologies and applications*. IGI Global, 2008. 612-618.

[15] [illegible] and Jingbing Li. "A new zero-watermarking algorithm resisting [illegible] attacks based on differences hashing." *Cybernetics and Information Technologies* 16.2 (2016): 135-147.

2022 International Conference on Smart and Sustainable Technologies in Energy and Power Sectors (SSTEPS)

Advanced Security for MANET using Ant Colony Optimization and Artificial Neural Network

Sangeeta Gulia
Department of CSE
Central University of Haryana
Mahendragarh, India - 123029
army.sangeeta46@gmail.com

Sarita Kumari
Department of CSE
RPS Groups of Colleges
Mahendragarh, India - 123029
saritanaveenkaliraman@gmail.com

Manish Kumar
Department of EE
Central University of Haryana
Mahendragarh, India - 123029
khanagwal.manish@gmail.com

Krishna Chaitanya A
Department of IT
Institute of Aeronautical Engineering
Hyderabad, Telangana, India- 500043
chaitui2004@gmail.com

***Abstract* - Manets are taught as a base for infrastructure wireless networks. Today main topics of research in Manets rotate around two main aspects- lifetime and security. This is just because of the wireless nature wherein vulnerability into network becomes comparatively much easier and the energy efficiency of all the nodes again is a crucial issue. The recent research is focused at enhancing security of Manets using the Ant Colony Optimization through Artificial Neural Networks thereby securing Manets from several intrusion attacks like worm hole and black hole attacks. The majority of optimization techniques work in past has been done using GA and now, the most recent algorithms like Particle swarm optimization, Tabu Search, ACO etc. have majorly reduced the limitations like premature convergence, which GA suffered from. Here, we will use ACO through Artificial Neural networks to create a robust system to increase the overall security of Manets. ANNs are the computational networks which are based on the behavior of biological neurons. These networks change through the information transferring through the network and provides help in pattern matching of inputs thereby guiding towards the most optimized output.**

Keywords* - *Genetic Algorithm (GA), Ant Colony Optimization (ACO), Artificial Neural Network (ANN), Particle Swarm Optimization (PSO).

I. INTRODUCTION

MANET stands for Mobile Ad hoc Network. It is nothing but a collection of mobile hosts that dynamically create a temporary network system for communication within nodes [1]. This network can have the capacity to configure itself every time when there is any movement occur in mobile node [2]-[3]. The connection between all the nodes are wireless so no infrastructure is needed. It is a static standalone network and can be able to connect with external networks or internet. In recent years, various algorithms and soft computing-based algorithms and frameworks have been incorporated [4]. These evolution-based algorithms are critical in self-adapting the framework under attack to expanding and new types of attacks, which are on the rise [5]. The Artificial Neural Network, also known as ANNs, is one of the computational intelligence algorithms analysed in this paper. It behaves similarly to biological neural networks in the human. In this paper, we demonstrate the ANN-based network structure used to counter DDoS attacks in the Audio - visual Internet of Things, as well as the architecture and incorporation of ANNs, as well as experimental research and findings that aid in drawing conclusions about ANN-based defence models [6].

A. *Blackhole Attacks*

Black hole attack is basically of two type's i.e. single and cooperative black hole attack which are based on the total number of hops which can be specifically involved in the attack. The MANET topology comprises seven modes in addition to the source and destination nodes expressed by the yellow and orange laptops, the red laptop serving as the black hole node, and the intermediate nodes on the left. The source is broadcasting an RREQ message [7]-[8]. The destination node regenerates the RREP message after receiving the RREQ packet. The black hole server transmits the regenerated RREP packet in addition to the FRREP with the maximum hop count, to the source node. As soon as the source node encounters the packet with both the maximum hope count, it begins sending data to the black hole node, believing it to be a destination node. Instead of forwarding the data to destination, the black hole node discards it [9].

II. ARTIFICIAL NEURAL NETWORKS

ANN is one of the AI methods which can provide a great tool for identifying malicious hops in MANETs. Learning ability and High computation rate with help of pattern presentation, prediction of unidentified or unknown patterns and flexibility offend the noisy patterns all are main advantages of ANN's [10].

Artificial neural network is nothing but a mathematical tool which id motivated by BNN. In most of the time a neural network acts as adaptive system reflexing its structure at the instant of a learning phase [11]. A neural network composed of an interlinked group of artificial neurons, and it can process all the information by using a connection oriented way of computation. NN are basically used for modeling highly

978-1-6654-6414-7/22/$31.00 ©2022 IEEE
DOI 10.1109/SSTEPS57475.2022.00093

complex relationships between outputs and inputs or to finding patterns in a data.
It is composed of so many "neurons" which can be co-operate to generate the desired output function.

A. *How Do a Neural Network Works?*

In order to construct a neural network, a vast number of artificial neurons, referred to as units, are arranged in a series of layers. Let's take a look at the various types of layers that can be found in an artificial neural networks.

Input Layer: As the name implies, it recognizes inputs in a variety of formats specified by the programmer.

Hidden layer: It does all of the calculations to reveal the hidden patterns and features.

Output Layer: The artificial neural network receives input and calculating the weight value of the inputs, as well as a bias. Output of a neuron is a combined function of weighted sum of inputs plus a bias

Input (x1 w1+x2 w2+x3 w3) + bias = Output (f(x1 w1+x2 w2+x3 w3 + bias))

The function of overall NN is just simply the calculation of outputs of all the neurons.

III. Ant Colony Optimisation

ACO is required for finding the solution of problems of all researchers using several kind of meta-heuristic techniques. It is basically a population based search oriented technique for finding the solution of so many difficult optimization problems (combinatorial). The main advantage of ACO is that it can solve optimization problems without any problem of premature convergence. ACO can be applicable on several optimization problems such as quadratic assignment, protein folding methods and in other implementations. It has been discovered that ant colony optimization (ACO) techniques can provide better results because they have Swarm Intelligence (SI) characterization, which is highly suitable for determining adaptive routing for such a volatile network. ACO algorithms are influenced by the foraging behavior of a group of ants, which can find the best path based on certain defined metric that is evaluated while the ants are moving. ACO routing algorithms employ simple agents known as artificial ants to establish optimal paths between both source and destination, which communicate indirectly via stigmergy. In light of the foregoing, we present a classification system of numerous ant colony algorithms, each with features and drawbacks in terms of performance.

ACO is motivated by the mechanism of the food search behavior of a real world ants and their capability to choose the best or optimized paths. In this, at initial state ants are randomly positioned and they start moving for searching of food and during returning to colony they leave their path towards that food source so that the rest of the ants in the colony won't go towards random paths, instead they follow the same path that was decided by the first group of ants. And the resulting accuracy of an Enhanced ACO is totally dependent on the parameter 'a' and the solution space. Space and Time complexity also decreased in Enhanced ACO.

Pseudocode

1. Generate i initial solutions, each one is associated to one ant
2. Initialize the pheromone trail
3. For Imax iterations repeat
   i. For each ant k = 1,, i do
      a. Modify ant k;s solution using the pheromone trail
      b. Apply a local search to the update a solution
      c. new initial solution to ant k using an intensification technique

   End For

   ii. Update the pheromone trail
   iii. Apply a diversification technique

   End For

IV. Implementation And Results

Here we can set antNET mode ON by default, this project doesn't work if we set antNET mode off. In this we remove all the problems of transmission and no calls are failed. We also try to find the current average number of the calls. Average is calculated according to simulation speed, concurrent number of calls. One more benefit of this we remove all the loops during transmission it decreases the chances of fail calls and it saves the time.

Fig. 1. Data Input

In Fig. 1 enter the input data into table. Set concurrent calls 6 and simulation speed x1, call duration is 170 and here node capacity is at 40. We can also decrease I/O speed also. After enter all input data then a click on the start button it will give the output. In output we see average of all concurrent calls and total number of calls mode and fails calls. For enter the new data we have to reset the table. After resetting the table, we enter the new data. Next we set concurrent calls 60, simulation speed x 10. Select the node 0 and click on to start button we will see the output of current average is 5.74 and total calls

mode is 101. None of the call is failed. We can see the results through graph of this result.

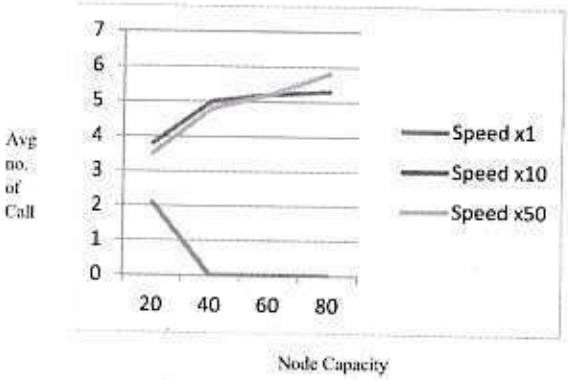

Fig. 2. Graph at Different Simulator Speeds

V. CONCLUSION

The AODV protocol security is breached by different types of attacks. Hubs in AODV discover routes through request-response cycles. By transmitting an RREQ message to all of its neighbor nodes, a node demands a route to a specific destination. When a node that receives an RREQ packet but does not have a pathway to the destination safely, the RREQ message is broadcast. It also remembers a backward to the source host that may be used to route future consideration to this RREQ. This procedure is repeated until the RREQ arrives at a node with a valid path to the destination. This node (which may or may not be the destination) needs to respond with an RREP packet. This RREP is send a packet through the transitional nodes reverse routes until it arrives the authentic requesting node. Also, basically role of local search is highly important for achieving better results. We highly believe on that ACO algorithms will evident on their efficiency when they will be properly applied on "ill-structured" problems for which it cannot be clear how we can apply on local search, or on extremely dynamic form of domains with only limited information is available.

REFERENCES

[1] Mohsin, Ahlam Hashim, et al. "A survey of energy-aware routing and mac layer protocols in manets: Trends and challenges." *Network Protocols and Algorithms* 4.2 (2012): 82-207.

[2] Harishankar, Sowjanya, et al. "E-MAnt net: An ACO-based energy efficient routing protocol for mobile ad hoc networks." *2015 IEEE 29th International Conference on Advanced Information Networking and Applications*. IEEE, 2015.

[3] Narayanan, Kumar, and Suresh Gnana Dhas Christhudas. "ACO-EEOLSR: enhanced energy model based link stability routing protocol in mobile ad hoc networks." *Journal of the Chinese Institute of Engineers* 39.2 (2016): 192-200.

[4] Vallikannu, R., A. George, and S. K. Srivatsa. "Autonomous localization based energy saving mechanism in indoor MANETs using ACO." *Journal of Discrete Algorithms* 33 (2015): 19-30.

[5] Singh, Gurpreet, Neeraj Kumar, and Anil Kumar Verma. "Antalg: An innovative aco based routing algorithm for manets." *Journal of Network and Computer Applications* 45 (2014): 151-167.

[6] Wang, Ya-li, et al. "Improved ant colony-based multi-constrained QoS energy-saving routing and throughput optimization in wireless Ad-hoc networks." *The Journal of China Universities of Posts and Telecommunications* 21.1 (2014): 43-59.

[7] Sharma, Chitra R., A. C. Suthar, and Yakuta Karkhanawala. "Energy constrained routing in MANET using ACO." *International Journal Of Innovative Research In Technology* 2.12 (2016).

[8] Abkenar, Gholamhasan Sajedy, Arash Dana, and Mohammad Shokouhifar. "Weighted probability ant-based routing (wpar) in mobile ad hoc networks." *2011 24th Canadian Conference on Electrical and Computer Engineering (CCECE)*. IEEE, 2011.

[9] Sharma, Shubham, and Anant Ram. "Energy Efficient Path Formation Approach in Wireless Ad Hoc Network." *2015 Fifth International Conference on Communication Systems and Network Technologies*. IEEE, 2015.

[10] Nancharaiah, [illegible] and [illegible] Mohan. "Modified ant colony optimization [illegible] enhance mantet routing in adhoc on demand distance vector." *2[illegible] International Conference on Business and Information Management (ICBIM)*. [illegible] 2014.

[11] Ram, M[illegible] and [illegible] Amit Chhabra. "Modified LA to Optimize the Performance of Mobile Ad Hoc Network." *IJESC*. DOI: 10.2015.350 (2015).

Lecture Notes in Networks and Systems 844

Harish Sharma
Antorweep Chakravorty
Shahid Hussain
Rajani Kumari *Editors*

Artificial Intelligence: Theory and Applications

Proceedings of AITA 2023, Volume 2

Springer

Investigating Role of SVM, Decision Tree, KNN, ANN in Classification of Diabetic Patient Dataset

Sarita Kumari and Amrita Upadhaya

Abstract Diabetes, which is a long-term ailment, is characterized primarily by high levels of sugar in the blood. It has been connected to a broad range of different types of complicated disorders, such as heart attack, renal failure, and stroke, among others. Almost 422 million people throughout the world were diagnosed with diabetes in 2014, and according to IDF Atlas 2021 report, 10.5% of the adult population (20–79 years) has diabetes, by 2045, IDF projections show that 1 in 8 adults approx. 783 million will be living with that disease an increment to 46% making it the most common metabolic. Logistic regression was used in traditional research to determine the characteristics that increase a person's likelihood of developing diabetes based on probability value and odds ratio. The authors utilize many classifiers to make predictions about diabetes patients, including NB, DT, AB, and RF. Twenty separate tests were conducted, each using one of three partitioning strategies. These classifier's effectiveness is measured by their accuracy and area under the curve. The overall accuracy rate of ML systems was 90.62% with conventional research. The K10 procedure combined LR-based feature selection with an RF-based classifier to obtain an ACC of 94.25% and an AUC of 0.95. The major goal of this work is to compare the performance of SVM, Decision Tree, KNN, & ANN on a dataset of diabetes patient classifications. The study's goals include improved accuracy and trustworthy results.

Keywords Diabetic patient · SVM · Decision tree · LR · KNN · ANN · Gaussian NB

S. Kumari (✉) · A. Upadhaya
Department of Computer Science and Engineering, Banasthali Vidiya Peeth, Rajasthan, India
e-mail: saritanaveenkaliraman@gmail.com

H. Sharma et al. (eds.), *Artificial Intelligence: Theory and Applications*, Lecture Notes in Networks and Systems 844, https://doi.org/10.1007/978-981-99-8479-4_32

CERTIFICATE

OF PUBLICATION

Karambir, Rajiv Kumar

for being an Author/Co Author of the Book : PLC AND SCADA SYSTEM under the ISBN : **978-81-19171-89-7** by **DREAMBOOK PUBLISHING**

RPS College of Engg. & Tech. IQAC BALANA (Mahendergarh)

05/09/2023

DATE

DreamBook Publishing

CEO SIGNATURE

Principal
R.P.S. College of Engg. & Tech
Balana Mohindergarh (HR.)

Samatrix.io

K.R. MANGALAM UNIVERSITY
THE COMPLETE WORLD OF EDUCATION

AIP Publishing

International Conference
on
Multidisciplinary Research & Innovations in Engineering
(MRIE-2023)

July 28-29, 2023

CERTIFICATE
FOR BEST PAPER

This is to certify that a paper entitled Analysing various parameters of photovoltaic cell: A Comprehensive Review presented by Kasambis at International Conference on Multidisciplinary Research & Innovations in Engineering (MRIE-2023) organized by School of Engineering & Technology, K. R. Mangalam University, Gurugram, Haryana is adjusted as Best Paper in the category

Convener
(MRIE-2023)

Program Chair
(MRIE-2023)

RPS College of Engg. & Tech. IQAC BALANA (Mahendergarh)

Principal
R.P.S. College of Engg. & Tech
Balana Mohindergarh (HR.)

MALAVIYA NATIONAL INSTITUTE OF TECHNOLOGY JAIPUR

Department of Chemical Engineering

International Conference

on

Advances in Chemical, Biological and Environmental Engineering (ICACBEE-2021)

(April 23-24, 2021)

Paper Code: *ICACBEE-2021-OP-086*

Certificate

Mr. Karambir Sheoran, Amity University, Jaipur, Rajasthan, India has **successfully participated** and **presented** a paper titled *"Parametric analysis of photovoltaic cells: A state of art review"* in the *"International Conference on Advances in Chemical, Biological and Environmental Engineering"* held during April 23-24, 2021 at MNIT Jaipur.

Co-Authors: ***Ashwani Kumar Yadav, Charanjeet Madan, Rajeev Sharma***

Dr. Manish Vashishtha
Conference Chairman

RPS College of Engg. & Tech. IQAC BALANA (Mohindergarh)

Dr. Sushant Upadhyaya
Conference Chairman

Principal
R.P.S College of Engg. & Tech
Balana Mohindergarh (HR.)

MALAVIYA NATIONAL INSTITUTE OF TECHNOLOGY JAIPUR

Department of Chemical Engineering

International Conference

on

Advances in Chemical, Biological and Environmental Engineering (ICACBEE-2021)

(April 23-24, 2021)

Paper Code: ***ICACBEE-2021-OP-086***

Certificate

Mr. Karambir Sheoran, Amity University, Jaipur, Rajasthan, India has **successfully participated** and **presented** a paper titled ***"Parametric analysis of photovoltaic cells: A state of art review"*** in the ***"International Conference on Advances in Chemical, Biological and Environmental Engineering"*** held during April 23-24, 2021 at MNIT Jaipur.

Co-Authors: ***Ashwani Kumar Yadav, Charanjeet Madan, Rajeev Sharma***

Dr. Manish Vashishtha
Conference Chairman

RPS College of Engg. & Tech. IQAC BALANA (Mohindergarh)

Dr. Sushant Upadhyaya
Conference Chairman

Principal
R.P.S College of Engg. & Tech
Balana Mohindergarh (HR.)

Mukand

ADVANCES IN ENGINEERING SCIENCE AND MANAGEMENT

Seth Jai Parkash Mukand Lal Institute
of Engineering & Technology
RADAUR - 135 133, DISTT. YAMUNA NAGAR (HARYANA)
www.jmit.ac.in

Title of the Book: Advances in Engineering Science and Management (Proceedings of the International Conference on Joint Modernistic and Innovative Technology)

First Volume - 2023

Editors

Dr. U. P. Singh, Ph:D. (B.H. U., Varanasi), Professor of Physics. Seth Jai Parkash Mukand Lal Institute of Engineering and Technology, Radaur (Yamunanagar), Haryana 135133.

Dr. R. S. Sharma, Ph.D. (N. I. T., Kurukshetra), Associate Professor, Electrical Engineering Department. Seth Jai Parkash Mukand Lal Institute of Engineering and Technology, Radaur (Yamunanagar), Haryana 135133.

Dr. S. K. Garg Ph. D (N. I. T., Kurukshetra) Director, Seth Jai Parkash Mukand Lal Institute of Engineering and Technology Radaur (Yamunanagar) Haryana 135133.

Disclaimer

The authors and editors are equally responsible for the contents published in this book. The publisher or editors don't take any responsibility for the same in any manner. Errors, if any, are purely unintentional and readers are requested to communicate such errors to the editors or publishers to avoid discrepancies in future.

E-ISBN: 978-93-5747-053-7

MRP: 220/-

Publisher, Printed at & Distribution by:
Selfypage Developers Pvt Ltd.,
Pushpagiri Complex,
Beside SBI Housing Board,
K.M. Road Chikamagaluru, Karnataka.
Tel.: +91-8861518868
E-mail:info@iiponline.org

IMPRINT: I I P Iterative International Publishers

Exploration of the FLC and ANFIS Controller's Performance with the Grid-Connected SPV Inverter

Ranjit Singh
Department of Electrical Engineering
JMIT, Radaur, Haryana 135133, India,

Rajiv Sharma
Department of Electrical Engineering
Quantum University, Roorkee, Uttarakhand

Abstract

In Solar Photovoltaic (SPV) systems, Maximum Power Point Tracking (MPPT) is a technology that increases the output power of the photovoltaic array regardless of the electrical characteristics, temperature, and irradiance of the load. In this study, a three-phase MPPT-controlled grid connected standalone solar photovoltaic systems is presented. The PV model is connected to the grid via a DC-DC boost converter. Additionally covered are the equation of the SPV cell, the three-phase PWM inverter, and the MPPT method for determining the maximum power coming from the SPV source. A comprehensive model is created to analyze the effects of various controllers on the semiconductor losses, junction temperatures, and sink temperatures of semiconductor devices.

Keywords: *IGBT, PI, PV*

I. Introduction

The utilization of non-conventional energy sources has significant advantages for the production of electricity. Utilizing non-conventional energy sources such as wind energy, biomass energy, solar energy, etc. allows for the production of electric energy. Sun energy in particular provides the advantages of pollution free, less maintenance costs, zero installation site restrictions, and no noise due to non-availability of moving parts. It is clear that each environment has a different Maximum Power Point (MPP), and that this peak power point changes as a function of sun light and temperature. This is due to the nonlinear relationship between the photovoltaic cell's output parameters. For solar photovoltaic (SPV) power generation to be highly efficient, it is essential to match the impedance of the source and load to each weather situation.Similarly The fact that current at maximum power (I_{MPP}), under different atmospheric conditions, is roughly finearly related to the current of the SPV array leads to fractional short circuit current (I_{SC}) [10]–[12]. The benefits of fuzzy logic controllers (FLC) include the ability to handle nonlinearity, cope with erroneous inputs, and do not require a exact mathematical model [13]–[17]. The adaptive neural fuzzy inference system [18]–[21] is another clever method. This research compares the Incremental Conductance MPPT algorithm for DC-DC boost converter based on Fuzzy logic controller and Adaptive neuro fuzzy inference system controller in order to increase efficiency and boost quality of output energy in grid connected SPV system. Similar to this, fractional I_{SC} results from the fact that current at maximum power (I_{MPP}), under various climatic conditions, is roughly linearly proportional to the I_{SC} of the SPV system [10]–[11]. FLC have a number of advantages, such as the capacity to deal with nonlinearity and incorrect inputs, and the lack of a precise mathematical model [13]–[17]. Another latest innovative technology is the ANFIS