RIK International Journal of Science and Technological Research (RIK-IJSTR) *Vol. 7 No. 1, January 2021*
ISSN: 2350-6310 (Print)
ISSN: 2350-543X (Online)

An Automated Diagnosis of Networks using Wireless Fidelity (Wi-Fi)

Mbato, Nnwobuike Robinson
Research Scholar
Department of Computer Science
Ignatius Ajuru University of Education
Rivers State
Nigeria

&

Onuodu, Friday Eleonu
Visiting Scholar
Department of Computer Science
University of Port-Harcourt
Rivers State
Nigeria

ABSTRACT

The management of a network is a difficult task regardless of the equipment that is part of the network. However, it is more difficult to manage networks when using devices and equipment from different manufacturers. Due to the use of a several devices on a network, the procedure of detecting an anomaly issues is usually more challenging because the circuits in the network have different single consoles under which they function. In this research, we propose an automated diagnosis system for networks using Wireless Fidelity (WiFi). The system depends solely on collection of packet traces upon reporting of a problem, and focuses on identifying faults and mis-configurations. The system starts by collecting a TCP packet trace of a known stream of data between the client device and the Internet Service Provider (ISP) router. This model yielded a better through put and detects all types of network faults identified in this research. The result from the model testing gave a performance score of 85% which is higher than the other techniques it was compared to. This research will be beneficial to network administrators, everyone that uses a network, researchers and students in the field of networking and network designers.

Keywords: Network, diagnosis, WiFi, Attenuation, Wireless network, TCP, packet tracing.

Introduction

Networks allow for information to sharing between devices that are connected together. Files, applications, printers and software are some of the resources that are also shared via the network platform [1]. The network basically comprises of the devices e.g. computers and the connectors such as hubs, routers, switch etc. that connect devices in the network. Networks can be either wired or wireless [2]. Either of these categories can be used to connect devices to the internet and to share information. They are several types of networks and they are classified based on size, topology and methods of connections. However, the Wireless Fidelity (WiFi) will be focused on in this study.

The Wireless Fidelity (WiFi) is a wireless network that is used to connect devices such as laptops, PCs, mobile phones etc to the internet at high speed without the use of a physical cable [3]. Radio signals are used to enable the connection to the internet. The WiFi can be used to facilitate automated diagnosis and troubleshooting of network problems especially short range networks where the connection is at high speed. Due to the increase in sophistication in the topology of the networks which are designed in recent times, it has become increasingly difficult to detect the exact fault in networks, especially in wireless networks. The WiFi is a handy tool that can be used to automate the process of network fault diagnosis irrespective of the level of sophistication of the network.

Statement of the problem

This study addresses some of the problems encountered in networks especially in the wireless network configuration. Some of these problems include Attenuation, reachability, Noisy network, link failure, Security policy violation, MAC buffer problems etc. these faults slow down the network performance and lead to low throughput of the network. Most times connectivity is completely lost due to the faults in the network. The WiFi however, will be used to implement an automated model that will diagnose these faults in the network.

Aim and Objectives

The aim of this study is to propose an automated diagnosis of networks using Wireless Fidelity. The specific objectives are:

i. To extensively explore the network topology for better understanding of the functionalities and its applications.
ii. To propose an automated diagnosis of network faults using Wireless Fidelity.
iii. To compare various network diagnosis models with our model, and evaluate the performance.

Significance of the Study

Networks have become a very important aspect of the lives of most people around the world. Most business thrives online and therefore need steady connection to the internet to carry out their businesses. These people will suffer a great loss if any point they lose connectivity due to faulty networks that are difficult to diagnose. Therefore this study will be beneficial to network administrators, everyone that uses a network, researchers and students in the field of networking and network designers.

Networks: A Review

A network can be defined as the connection of various devices together for the goal of sharing information and resources [1]. The benefit of networking can be clearly seen in terms of security, efficiency, manageability and cost effectiveness as it allows association between users in a broad range. Fundamentally, network is made up of hardware component which include the computer, hubs, switches, routers and other devices which make up the network infrastructure. These components play a significant function in transferring data from one point to another using different medium such as radio waves and wires [1].

Classifications of Networks

Networks are classified basically based on their sizes, and these include the Personal Area Network (PAN), Local Area Network (LAN), Virtual Private Network (VPN), Metropolitan Area Network (MAN) and Wide Area Network (WAN).

a. Personal Area Network (PAN)

PAN is a kind of network used to connect devices and computers inside a relatively small place to other networks. For example computer can be connected to other devices like printer, fax, and telephones with personal computer where usually those kinds of communications can be wire, but most of new PAN communication depends on wireless ability by using Bluetooth or infrared. Which enable communication with limited range, and enable user move fixable around the range. But on the other hand, data transfer is insecure over devices where electromagnetic waves transfer over public media [4] [5].

b. LAN

Local Area Network (LAN) applied in limited geographical area like universities and laboratory, home, and schools. Ethernet usually used to communicate between devices in LAN, where it is easier to create a network by using phone cables and other power lines. Other advantages of this kind of networks are creating some group of these devices by creating some subnet networks. Usually LAN networks can be transfer data between devices by using other communication devices which is called switching system or called switch system, (switch, hub) where switch contain three layers only [6] [7].

c. VPN

VPN represents one category of networks that can employ some networks to connect with other computers where X.25 developed for commercial services and produced TCP/IP networks [6]. Nowadays, computer networks developed in different categories and in other classes from LAN networks and other for WAN networks. Moreover direction of development for software where new protocols design for transfer data between devices in additions other classes for peripherals devices that support network system [8][9].

d. MAN

This network represents the middle geographical extend between LAN and WAN. MAN could be used to connect as large as a city or a large area. MAN is large than LAN and small than WAN. Also large university used this kind of network to communicate between labs and offices. Usually MAN did not belong to single organization but sometimes to more than one. Which represent high speed network can be used where it can use same ability of LAN and less size than WAN. One of the famous examples of MAN is Distributed Queue Dual Bus (DQDB), which is defined by Electrical and Electronics Engineers IEEE 802.6 [10]**.**

e. WAN

This is a connection between devices in the world where information can be transferred from any device in any country to other device in any other side of the world. It applies in a large scale geographically. Where usually governments used this network to communicate between its institutions, more over global businesses can employ this kind of communication to support connection between company parts, and also marketing for its stuff [11].

Networks can also be classified based on the topology. This describes the way which the devices are connected in the network. Based on topology, the classifications is star topology, ring topology, point-point connection, hierarchical, BUS, Fully connected network, hybrid topology.

a. **Point to Point Connection:** this is the simplest kind of communication between two devices. Both devices are connected directly to one computer without any branches of connections. The main disadvantage of this method is connection will fail if a wire is disconnected and this will disable the connection between other [12].

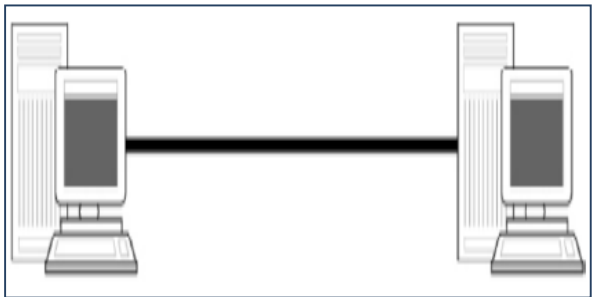

Fig. 1 Point to Point Connection (Source: [2])

b. **Bus Connection:** Here, only one cable is used to connect more than two devices using a single link. Usually each device has ability to send and receive data over that bus and this reduces cost of connection. On other hand, if two devices decide to send data at same time then data will be lost due to collision. At the end of bus there is a terminator which is used to absorb the remaining data. On other hand if collision occurs, each device will wait a random amount of time then resend data again. So new technology used to reduce the problem of collision is by using sensor, where each device has a sensor at the end of lower level [13].

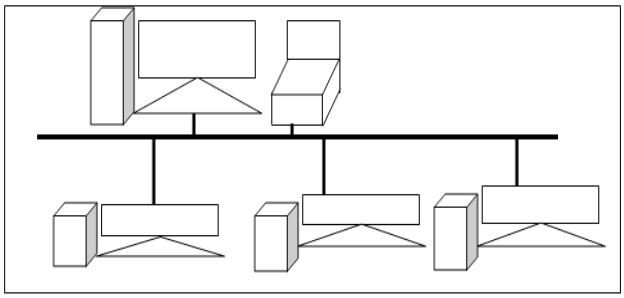

Fig. 2 Bus Connection (Source: [2])

c. **Star Topology:** in this network a switch is used to organize connection between devices where information is first sent from sender to the switch and then from the switch to receiver, and any connection must follow this process. So if any problem occurs in any node, the network will still function normally. Moreover if a hub or switch wants to send data only, it can broadcast information over that network. On the other hand, if a hub stops working the whole network will be shut down. However, the star network has a better performance than the BUS topology [13].

d. **Hierarchical Topology:** this is also called tree network topology. Information is sent from an upper level to a lower level. Each node has three component two sons and one parent. If data send from top to down, then each root node decides which son can receive data .The main advantage of this network is the ability to divide and still keep working [14].

e. **Fully Connected Network:** this is a kind of network where a node is connected to all nodes around it, the number of connected node is given by n(n-1)/2 where n is number of nodes. The main advantage of this network is that there is no collision between nodes [15].

f. **Ring Topology:** nodes connected like a ring between one other and each node has same ability like next one to send packet over network. If any node want to send data over network it will wait until he receive token packet after that it will catch token packet and keep it, then start streaming its data over network until its finish and data will take around when it receive last packet sent it then token can be released. Ring topology is very organized special where collision can't be created between node data where only one user can send data at time if it has token. This network can be used to transmit large packets of data [16].

Network Faults

There are various faults that occur in networks either due to their connections or the devices used in the connection. Some of the faults are explained below:

a **Physical Fault:** Physical fault is hardware failure and the form for this kind of failure is diverse. It is also one of the more common faults for network equipment and relatively easy to solve. The most common form of network is unstable connection, sometimes even complete disconnected.

b **Port Fault:** Port fault mainly has two cases: unstable port and port failure. Screening methods: port usage conditions will be reflected to the other devices signal light. As a result, fault area and the reason can be determined by observing the status of these signal lights. In addition, other ports can be used for testing. If communication is normal, which means there is a problem for it; if the communication is failed, port fault is ruled out.

c **Switches or Routers Breakdown:** Switch or router fault refers to equipment damage, resulting in abnormal work and network fault. Screening methods: determine whether the switch or router equipment in good condition, and there are two simple ways: first, the method of observation. Observe indicator light, in normal condition, switches and routers light should be green; otherwise, the equipment can be judged as damaged. Second is replacement method. The Internet and computer in normal use can be used to connect devices, if the communication restore to normal, it means the equipment is normal; if the communication is still failed, the port of switch or router should be screened.

d **Network Card Fault:** Network card fault belongs to host hardware failure. As network terminal, network card failure is also an important cause of network failure. As the network card is usually installed within the host, its fault has certain concealment. In addition, the network adapter failure also has diverse forms, such as loose network card, network card hardware failure, and host card slot fault and so on, which can lead to abnormal work of network card.

e **Logic Fault:** Logical failure is software failure which is corresponding to the physical fault. When computer has logic problems, the network speed is quick and slow sometimes, bringing adverse effects to web browsing. Physical fault identification and screening is “visible and tangible”, and therefore is relatively simple. Logical fault cause is relatively complex, so the difficulty for screening is higher. These kinds of failures often need to rely on specialized technical personnel to help solve. It mainly includes the host logical fault, wrong host network address parameter setting, improper host network protocols or services installation, improper network card driver installation, some important process or port closed, and so on.

Techniques for Diagnosis of Networks

The need for an enhanced mechanism that can match the increasing rise in networked systems cannot be over stressed. The mechanisms are needed to intelligently detect problems in network configurations diagnose the cause of such failures. To attain true self-healing networks, there is a need for mechanisms that can repair these failures and guarantee service availability by providing optional of communication after the detection. Some of the mechanisms that have been proposed by researcher over the years are explored below:

- Yuanyuan [17] proposed a monitoring scheme for mobile networks based on the use of rules and decision tree data mining classifiers to upgrade fault detection and handling. The aim of their work was to develop optimization rules that will enhance the detection of anomaly. Additionally, they implemented a monitoring scheme that based on Bayesian classifiers which will isolate faults and localize them. They used data learning techniques to train the system to learn network fault rules. They concluded that this technique showed a high performance accuracy during network troubleshooting when tested. However, they were not able to examine the business decisions that underlie network optimization efforts on the part of network providers.
- Samira et al [18] proposed fault detection in cellular networks using Support system's data. Relevant quality indicators in live mobile communications were considered. They presented an automated combined detection and diagnosis framework to spot the root causes of faults that are noticed in the network. Unsupervised clustering was the proposed solution of both traffic and signaling (continuous) key performance indicators for diagnosis. This makes it immune to the human error in the modeling phase. The system also allowed effective encapsulation of expert knowledge as they relate clusters to original causes in the design phase. Detailed analysis of fault detection, the clustering schemes and the diagnosis are provided using operations support systems data of a real cellular network.
- Singh et al [19] proposed DYSWIS for automated diagnosis of network issues. They introduced DYSWIS ("Do you see what I see") which relies on observing the system from multiple points in the network. Our system consists of detection nodes and diagnosis nodes. Detection nodes detect failures by passive traffic monitoring and active probing. Diagnosis nodes determine the cause of failures using historical information about similar failures and by performing active tests. They were based on a rule engine and represent network dependency relationship encoded as rules. They presented our prototype system which considers network components present in a VoIP network and show the feasibility of our solution. However, they lacked instrumentation of applications to detect and report failures in order to trigger diagnosis.
- Chhaya et al [20] proposed Wireless Sensor Network in Smart Grid. WSN is a cost effective solution for monitoring, control, measurement and fault diagnosis in various domains of smart grid network. A sensor node mainly contains sensors, memory, processor, power supply, transceiver and actuator. Sensors are used to sense various quantities like humidity, temperature, current, etc. Generally, WSN nodes are battery powered. Small sensor nodes collectively form a sensor network which is used for remote wireless communication in HAN, NAN and WAN. Large scale deployment of sensor nodes can be used to communicate the conditions of various generation, transmission and distribution units. Wireless sensor nodes can provide economical solution for smart microgrid monitoring which facilitates high penetration of renewable energy sources.
- Akinrinlola [21] proposed fault detection and diagnosis using trace driven simulation. They stated the necessary and sufficient conditions for being able to detect which node is faulty, and propose a diagnosis algorithm, a system that employs online

trace-driven simulation on the basis of diagnosability definitions and theoretical studies developed for timed and hybrid automata in the computer science community. They assumed that their interface with the network was a gateway node that accepts ping commands (control input), and replies with pong responses after a time delay that we can measure (observed output). They focused on a part of the general network management problem, namely fault detection, isolation, and diagnosis. It proposes a system that employs online trace-driven simulation as a diagnostic tool for detecting faults and performing root cause analysis.

Wireless Fidelity (WiFi)

Wi-Fi stands for "Wireless Fidelity" and was used to describe Wireless LAN (WLAN) products that are based on the IEEE 802.11 standards. Wi-Fi uses both single carrier direct-sequence spread spectrum radio technology and multi-carrier OFDM (Orthogonal Frequency Division Multiplexing) radio technology. These regulations then enabled the development of Wi-Fi and its onetime competitor HomeRF, and Bluetooth. Wi-Fi's first wireless products were brought on the market under the name WaveLAN with speeds of 1 Mbit/s to 2 Mbit/s and standards designed as IEEE 802.11b, and 802.11a [12]. Wi-Fi is owned by the Wi-Fi Alliance which is a consortium of separate and independent companies agreeing to a set common interoperable products based on the family of IEEE 802.11 standards.

Wireless Fidelity (Wi-Fi) is a genuine motorization structure that uses radiofrequency to impart data through the air. With a hidden speed of 1 Mbps to 2 Mbps, it sends data with a repeat band of 2.4 GHz appropriately developing the possibility of repeat division multiplexing advancement and ranges from 40-300 feet. The devices are on a very basic level controlled through a microcontroller. The data is sent from the PC over Wi-Fi and will be gotten by a Wi-Fi module related with the microcontroller which scrutinizes the data and picks the trading technique for the electrical contraptions related with it through Relay Boards. A part of the advantages of WiFi development are:

a In neighboring or removed spots, distant center points can be mounted all finished. These assistants in enlarging the covered locale.
b System is flexible and the enlargement is basic as it needn't waste time with any real assistance.
c Placement of far off center points is uncommonly basic as it will in general be presented at any territory, for instance, glass structures or recorded structures.
d Any number of phones can be affixed to the structure wherever around the world.

Related Work

- Samhat et al [23] proposed automated trouble shooting in WLAN networks. They zeroed in on robotized analysis of shortcomings in WLAN organizations and proposed a structure dependent on Bayesian Networks to relate flaws to indications. Up-and-comer rundown of deficiencies and manifestations for the determination were proposed and the way to build the analysis model was portrayed. To show the proposed approach, a few

outcomes were inspected dependent on measurements from WLAN network test system. Be that as it may, they couldn't utilize insights from genuine WLAN network in the learning stage.

- Bakare and Minah-Eeba [3] proposed A Comprehensive Review of Wireless Fidelity (Wi-Fi) Technology in Nigeria. They talked about the latest thing and future exploration headings that could prompt major changes in remote access arrangement, that is, regions of future reevaluations incorporates: Li-Fi, WiMAX, Super Wi-Fi, Wi-Fi confirmed and so on nonetheless, they couldn't proffer answer for any of the difficulties recognized.
- Cheng et al [24] presented a set of modeling techniques for automatically characterizing the source of such problems. Specifically, the zeroed in on information move postpones one of a kind to 802.11 organizations, media access elements and portability the board inactivity. Through a mix of estimation, induction and displaying we remake wellsprings of deferral from the actual layer to the vehicle layer just as the connections among them. They exhibited their methodology utilizing thorough hints of remote movement in the UCSD Computer Science building.
- Rajashree et al [25] presented a design and prototype implementation of new home automation system that uses Wi-Fi technology as a network infrastructure connecting its parts. With the assistance of a web worker and a LAN association the framework gives a versatile and a wide reach coverable gadget. The framework is profoundly cutting-edge as it utilizes a less expensive Wi-Fi association and a worker that can store information. Clients and framework overseer can locally (LAN) or distantly (web) oversees and control framework code. Hence, an exceptionally mechanized framework is accessible to the client. The framework is made sure about as the client needs to enter secret word and that isn't known to any gatecrashers.
- Vian [26] proposed an automated approach to diagnose the performance stalls in networked systems. Stream diagnoser needs as meager as two pieces of data for every module to make a determination: one to demonstrate whether the module is effectively preparing information and one to show whether the module is looking out for its wards. To help their examination, Flow Diagnoser was actualized in two particular conditions: an individual host's organizing stack, and an appropriated streams handling framework.
- Patro et al [27] presented a measurement study of wireless experience in a diverse set of home environments by deploying an infrastructure, called WiSe. The foundation comprises of OpenWrt-based Access Points (APs) that have been offered away to occupants for nothing to be introduced as their essential remote access instrument. These APs were arranged with our particular estimation and observing programming that speaks with their estimation regulator through an open API. They gathered remote execution follows from 30 homes for a period more than a half year. To examine the qualities of these home remote conditions, they built up a basic metric that gauges the imaginable TCP throughput various customers can anticipate dependent on current channel and ecological conditions. With this framework, they gave various quantitative perceptions, some of which are narratively perceived in our locale. For instance, while a lion's share of connections performed well more often than not, we noticed instances of helpless customer experience about 2.1% of the complete time.

- Nwabueze and Akaneme [28] explores the Wi-Fi broadband wireless network technology, its uses, advantages and disadvantages, comparison with other broadband wireless networks and integration with WiMAX network. However, they could not implement an actual model that can be used to diagnose network faults.
- Tong et al [29] presents a survey on troubleshooting with a special concentration on network issues. The fundamental commitment of this study is a definite examination of best in class identified with network issues investigating which assesses their advantages and disadvantages. Also, these exploration works are characterized into certain classifications to give the helpful rule to investigating research.
- Mathis et al [30] they described a tool to diagnose network performance problems commonly affecting TCP-based applications. The apparatus, pathdiag, runs under a web worker structure to furnish non-master network clients with a single tick symptomatic testing, tuning backing and fix guidelines. It analyzes numerous reasons for helpless organization execution utilizing Web100 measurements and TCP execution models to conquer the absence of in any case recognizable side effects. Be that as it may, they couldn't analyze remote organization deficiencies.
- Barros et al [31] proposed a model diagnosis for network communication faults. It was analytic framework for correspondence flaws and a demonstrative framework for design blunder. The demonstrative of setup mistake can identify and alarm the organization supervisory group for design blunders (irregularities between directing tables, for instance) that can cause other correspondence issues or execution bottlenecks. The analytic of correspondence issue could decide an organization component (of a negligible arrangement of them) that are causing correspondence mistake, in light of either the loss-of-signal alerts or on an explicitly developed inquiry module that tests the openness of organization components intermittently. The two subsystems were tried on misleadingly developed organizations.

Proposed Technique

After a broad examination, we propose a robotized determination for networks utilizing WiFi to address the previously mentioned issues. The proposed framework is insightful induction technique for diagnosing network issues utilizing TCP bundle follows which we call the Automated Network analysis framework. The framework analyzes shortcomings in WiFi network associations. The framework depends just on assortment of parcel follows after announcing of an issue, and spotlights on recognizing issues and mis-designs. The framework begins by gathering a TCP parcel hint of a known stream of information between the customer gadget and the Internet Service Provider (ISP) switch. This is started by the client through an extraordinarily made page that enacts the follow assortment application. This follow is then examined by the smart framework, which contains two AI prepared classifiers. Accepting that the entrance worker is advanced for the association, execution issues experienced by the end client can be credited to either the entrance connection or customer gadget.

Since the framework is intended to analyze customer gadget issues, a test is first performed to recognize whether the exhibition issue is because of flawed admittance joins. The TCP parcel follow is passed to the primary phase of the framework, the Link Problem Detection (LPD) classifier that reports whether an entrance connects is working true to form. On the off chance that the LPD classifier verifies that the entrance interface is broken, at that point the connection issues ought to be settled prior to endeavoring to analyze any customer shortcomings. We have left the programmed finding of the entrance connect issues for future work. On the off chance that the connection is recognized to be sound, the bundle follow is passed to the Client Fault Diagnostic (CFD) classifier to distinguish the specific main drivers of any issues in the customer gadget.

Algorithm of the Proposed System

The algorithm of the proposed system can be illustrated below:

STEP 1: Collect a Packet Trace
STEP 2: Set Link Type
STEP 3: Run LPD Classifier
STEP 4: Link Problem Detected?
THEN
Solve Link Problem
STEP 5: Collect a New Packet Trace
ELSE
Run CFD Classifier over the Trace
STEP 6: Client Problem Identification Report

Comparison of Different Diagnosis Techniques

Table 1. Model Comparison

S/N	Author	Year	Technique	Performance	Advantage	Disadvantage
1	Van	2018	Flow Diagnoser	30%	Requires as little as two bits of information per module to make a diagnosis	Cannot diagnose faults in WiFi Networks
2	Samhat et al	2016	Bayesian Networks	40%	-	-
3	Samira et al.	2012	Support system's data.	70%	Identify root causes of faults occurred in the network.	-
4	Mbato	2020	TCP Packet Tracer	85%	Quick diagnosis of faults intelligently without human intervention.	-

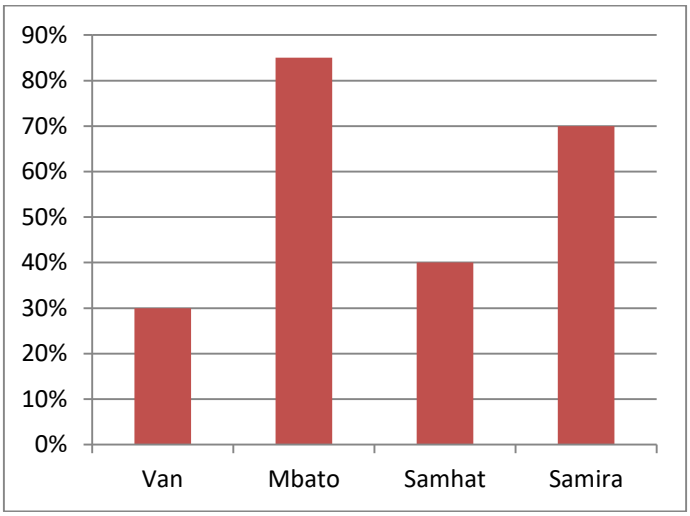

Fig. 3: Model comparison Chart

Conclusion

In this work, we have proposed and evaluated an intelligent model, an automated diagnostic system that uses an intelligent inference based approach of TCP packet traces to identify artifacts created by various faults. The model detects the faults in WiFi networks using packet tracing. The WiFi networks are high speed networks that allow connection to the internet. The Model detects faults by tracing packets that are sent over the network. This model is more efficient than the other models used for network diagnosis and will yield better throughput when applied to wireless networks.

References

[1] A.M. Saravan. "Introduction to Networking Research Gate Publication. pp. 1-12. Mar. 2012.

[2] B. Badr, and B. Christian. "Network Overview". IJWCN, vol. 5, issue 2. 2013.

[3] B.I. Bakare, and W. Minah. "Comprehensive Review of Wireless Fidelity (WiFi) Technology in Nigeria" Vol. 13, No. 3, 37-42.

[4] I. Howitt and J. A. Gutierrez, "IEEE 802.15. 4 Low Rate wireless Personal Area Network Coexistence Issues," in *Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE,* 2003, pp. 1481-1486.

[5] T. M. Siep, I. C. Gifford, R. C. Braley, and R. F. Heile, "Paving the Way for Personal Area Network Standards: an Overview of the IEEE P802. 15 Working Group for Wireless Personal Are a Network s," *Personal Communications, IEEE,* Vol. 7, pp. 37-43, 2000.

[6] N. J. Boden, D. Cohen, R. E. Felderman, A. E. Kulawik, C. L. Seitz, J. N. Seizovic, and W.-K. Su, "Myrinet: A Gigabitper-second Local Area Network," *Micro, IEEE,* Vol. 15, pp. 29-36, 1995.

[7] B. Brown and S. A. Chowdhury, "Apparatus and Method of Monitoring the Status of a Local Area Network," ed: Google Patents, 1993.

[8] M. S. Pegrum, D. Jamieson, and M. Yuen, "Virtual Private Networks," ed: Google Patents, 2003.

[9] D. H. Cho, J. H. Song , M. S. Kim, an d K. J. Han , "Performance Analysis of the IEEE 802.16 Wireless Metropolitan Area Network," in *Distributed Frameworks for Multimedia Applications, 2005. DFMA'05. First International Conference on*, 2005, pp. 130-136.

[10] B. Kahle and A. Medlar, "An Information System for Corporate Users: Wide Area Information Servers," *Online*, Vol. 15, pp. 56-60, 1991.

[11] M. Ripeanu, "Peer-to-peer Architecture Case study: Gnutella Network," in *Peer-to-Peer Computing, 2001*.

[12] Wi - Fi -Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/WiFi.

[13] H. Tangmunarunkit, R. Govindan, S. Jamin, S. Shenker, and W. Willinger, "Network Topology Generators: Degree-based vs. Structural," in *ACM SIGCOMM Computer Communication Review*, 2002, pp. 147-159.

[14] Y. Shavitt, "Routing through Networks with Hierarchical Topology Aggregation," *Journal of High Speed Networks*, Vol. 7, pp. 57-73, 1998.

[15] M. Jelasity and O. Babaoglu, "T-Man: Gossip-based Over lay Topology Managemen t," *Engineering Self- Organising Systems*, pp. 1-15, 2006.

[16] C. S. Kang, E. K. Park, and J. H. Herzog, "Hybrid-token Ring: A Load Sharing Local Area Network," *Computer Communications*, Vol. 14, pp. 525-533, 1991.

[17] C.Y. Yuanyuan. General Identification of Solutions of Computer Network Faults. 6th International Conference on Management, Education, information and Control. Pp. 0657-0660. 2016.

[18] E. Rozaki. Design and Implementation for Automated Network Troubleshooting using Data Mining. *International Journal of Data Mining and Knowledge Management*. Vol, 3 N0.9. pp. 9-27. May 2015.

[19] R. Samira, R. Hamidreza, A. Payam, N. Hamidreza and L. Farshad. Automatic Fault Detection and Diagnosis in Cellular Networks ising Opeartions Support System's Data. IEEE/IFIP Network Operation and Management Symposium (NOMS 2016).

[20] K.V. Singh, H. Schulzrinne, and K. Miao. DYSWIS: An Architecture for Automated Diagnosis of Networks. Researchgate Publications. Pp. 1-8. 2017.

[21] L. Chhaya, P.Sharma, G. Bhagwatikar and A. Kumar. Wireless Sensor Networks Based on Smart Grid Communications: Cyber Attacks, Intrusion Detection System and Topology Control. *Electronics.* Vol. 6 No. 5, pp. 1-22. Oct 2016.

[22] I.B. Akinrinlola. Fault Detection and Diagnosis over A Wireless Network (Using Trace Dreiven Simulation). *Scholarly Journal of Scientific Research and Essay*. Vol. 4 No. 8, pp 151-161. Oct. 2015.

[23] A. Samhat, R. Skehill, and Z. Altman. Automated Troubleshooting in WLAN Networks. *European Celtics Gandalf Project.* Pp. 1-5. 2016.

[24] Y. Cheng, M. Afasyer, S. Savage, and G,M. Voelker. Automating Cross-Layer Diagnosis of Enterprise Wireless Ntework. *SIGCOM'07.* Pp. 1-12.

[25] C. Rajashree, A. Sarkar, S. Agarwal and A. Nath. Proposed Design and Implementation of a Home Automation System Based on WiFi. *International Journal of Research Studies in Computer Science and Engineering (IJRSCSE).* Vol. 3 Issue 3, pp. 18-26. 2016.

[26] T. Vian. Automated Diagnosis of Network Performance Problems. Ugandan Technology and Management University. Pp. 1-14. 2019.

[27] A. Patro, S. Govindan, and S. Banerjer. Observing Home Wireless Experience Through WiFi Aps. Researchgate Publications. Pp. 1-12

[28] C.A. Nwabueze and S.A. Akaneme. Wireless Fidelity (WiFi) Broadband Network Technology: An Overview with other Broadband Wireless Network. *Nigerian Journal of Technology.* Vol. 28 No.1, pp 71-78. Mar 2009.

[29] V. Tong, H.A. Tran, S. Souihi and A Mellouk. Network Troubleshooting: Survey, Taxonomy and Challenges. *Researchgate Publications*. 1-7. 2011

[30] M. Mathis, J. Heffner, p. O'Neil and P. Siensen. Automated TCP Diagnosis. LNCS4979. Pp. 152-161.

[31] L.N. Barros, M. Lemos, B. Volnys, and W. Jacques. Model Based Diagnosis for Neywork Communication Faults. AAAI Technical Report WS-99-03 Compilation, pp. 57-62. Jul. 1999.