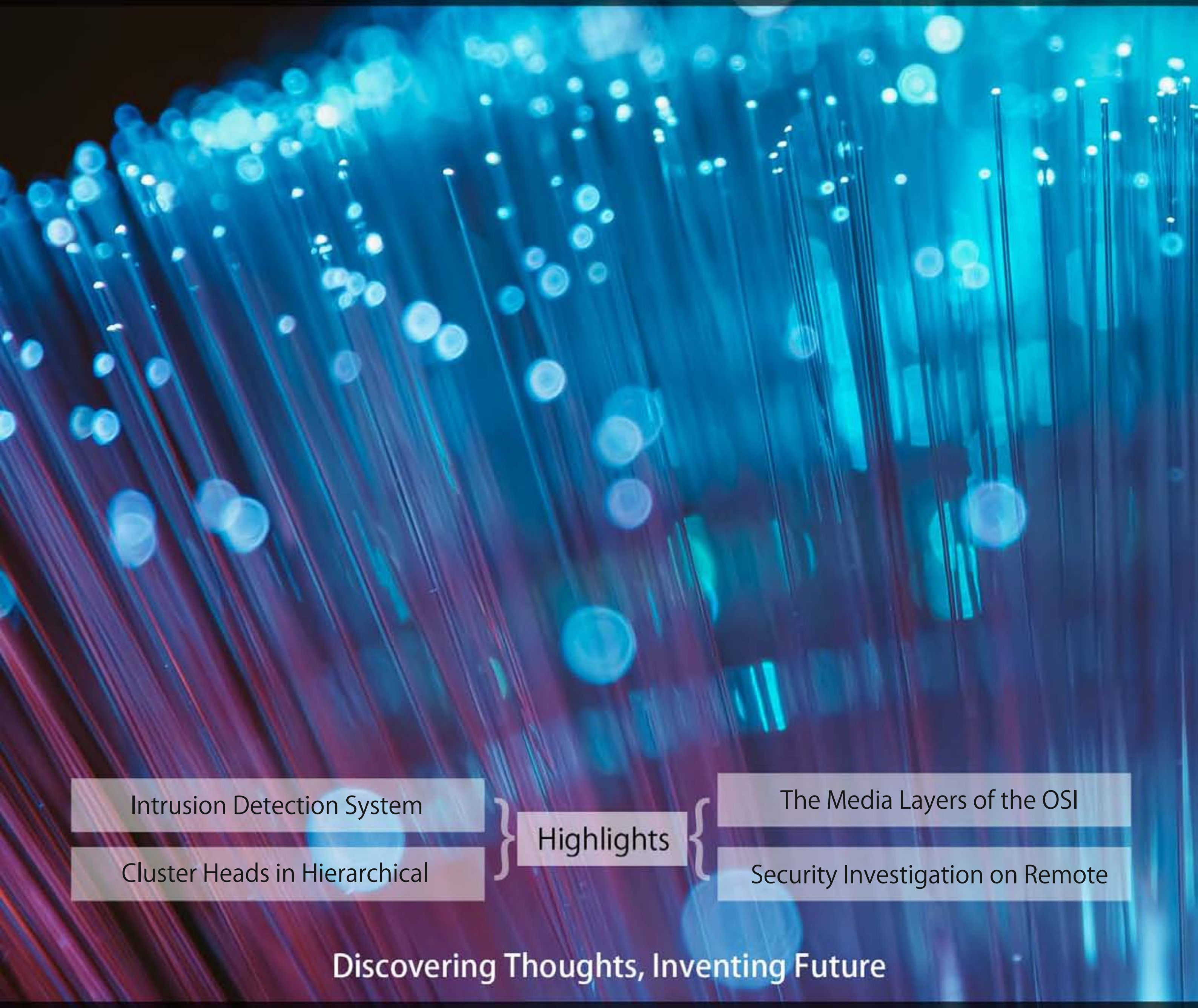
Online ISSN : 0975-4172
Print ISSN : 0975-4350
DOI : 10.17406/GJCST

Global Journal

of Computer Science and Technology: E

Network, Web & Security



Highlights

- Intrusion Detection System
- Cluster Heads in Hierarchical
- The Media Layers of the OSI
- Security Investigation on Remote

Discovering Thoughts, Inventing Future

VOLUME 20 ISSUE 1 VERSION 1.0

Global Journal of Computer Science and Technology: E
Network, Web & Security

Global Journal of Computer Science and Technology: E
Network, Web & Security

Volume 20 Issue 1 (Ver. 1.0)

Open Association of Research Society

The opinions and statements made in this book are those of the authors concerned. Ultraculture has not verified and neither confirms nor denies any of the foregoing and no warranty or fitness is implied.

Engage with the contents herein at your own risk.

The use of this journal, and the terms and conditions for our providing information, is governed by our Disclaimer, Terms and Conditions and Privacy Policy given on our website http://globaljournals.us/terms-and-condition/menu-id-1463/

By referring / using / reading / any type of association / referencing this journal, this signifies and you acknowledge that you have read them and that you accept and will be bound by the terms thereof.

All information, journals, this journal, activities undertaken, materials, services and our website, terms and conditions, privacy policy, and this journal is subject to change anytime without any prior notice.

Incorporation No.: 0423089
License No.: 42125/022010/1186
Registration No.: 430374
Import-Export Code: 1109007027
Employer Identification Number (EIN):
USA Tax ID: 98-0673427

Global Journals Inc.

*(A Delaware USA Incorporation with "Good Standing"; **Reg. Number: 0423089**)*

Sponsors: *Open Association of Research Society*
Open Scientific Standards

Publisher's Headquarters office

Global Journals® Headquarters
945th Concord Streets,
Framingham Massachusetts Pin: 01701,
United States of America
USA Toll Free: +001-888-839-7392
USA Toll Free Fax: +001-888-839-7392

Offset Typesetting

Global Journals Incorporated
2nd, Lansdowne, Lansdowne Rd., Croydon-Surrey,
Pin: CR9 2ER, United Kingdom

Packaging & Continental Dispatching

Global Journals Pvt Ltd
E-3130 Sudama Nagar, Near Gopur Square,
Indore, M.P., Pin:452009, India

Find a correspondence nodal officer near you

To find nodal officer of your country, please email us at *local@globaljournals.org*

eContacts

Press Inquiries: *press@globaljournals.org*
Investor Inquiries: *investors@globaljournals.org*
Technical Support: *technology@globaljournals.org*
Media & Releases: *media@globaljournals.org*

Pricing (Excluding Air Parcel Charges):

Yearly Subscription (Personal & Institutional)
250 USD (B/W) & 350 USD (Color)

Editorial Board

Global Journal of Computer Science and Technology

Contents of the Issue

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 20 Issue 1 Version 1.0 Year 2020
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 2249-4596 & Print ISSN: 0975-5861

Modeling on Body Delay Tolerant Network Sink Locality of Wireless Body Area Networks for Different Body Postures

By Anthony M. Mile
Jomo Kenyatta University

Abstract- Due to the recent advancements in the field of wireless communication and Wireless Sensor Networks, the Wireless Body Area Networks (WBANs) have become an area of concern for researchers. In military operations, patient monitoring, sports field, among other wireless body area networks is used for real time monitoring and smart sensing for eHealth operations. In these WBAN, disconnections between the body sensors occur quite often and sometimes of significant duration due to the postural mobility nature of the human. These consequently affects the efficiency of the entire network hence the need for Delay Tolerant Network (DTN). The DTN minimizes delays and adapts itself to cope with long delays if they occur. One of the vital mechanisms that can be employed to enhance the efficiency of the network is to determine the optimal postural locality of the sink node.

Keywords: *wireless sensor network (WSN), wireless body area network (WBAN), delay tolerant network (DTN), sink locality.*

GJCST-E Classification: *J.m*

Modeling on Body Delay Tolerant Network Sink Locality of Wireless Body Area Networks for Different Body Postures

Anthony M. Mile

Abstract- Due to the recent advancements in the field of wireless communication and Wireless Sensor Networks, the Wireless Body Area Networks (WBANs) have become an area of concern for researchers. In military operations, patient monitoring, sports field, among other wireless body area networks is used for real time monitoring and smart sensing for eHealth operations. In these WBAN, disconnections between the body sensors occur quite often and sometimes of significant duration due to the postural mobility nature of the human. These consequently affects the efficiency of the entire network hence the need for Delay Tolerant Network (DTN). The DTN minimizes delays and adapts itself to cope with long delays if they occur. One of the vital mechanisms that can be employed to enhance the efficiency of the network is to determine the optimal postural locality of the sink node. The human body experiences postural mobility leading to the WBAN topological disconnections. A WBAN model was created for illustrating and capturing on-body these disconnections. In this paper, the Omnet++ simulation tool was used to determine the postural locality of a sink node of a human body. The results showed that the waist position of the coordinator outperforms other positions based on average delay and energy consumption. By determining the best postural locality of the sink node, among other factors, the performance and lifetime of the WBAN can be improved.

Keywords: wireless sensor network (WSN), wireless body area network (WBAN), delay tolerant network (DTN), sink locality.

I. Introduction

As society advances, smart healthcare services become necessary to tackle health challenges. For instance, an intelligent healthcare monitoring service can be deployed to more effectively monitor a patient from anywhere at any time (Chen et al., 2005; Darkins et al., 2008; Quwaider & Biswas, 2008; Lv et al., 2010; Quwaider & Biswas, 2010; Yi et al., 2016). There has been significant research which has been carried out in the last decades by both academia and industry targeted towards improved adoption and effectiveness of this technology development (Prameela & Ponmuthuramalingam, 2016; Gowtham & Ahila, 2017; Quwaider & Biswas, 2010; Chen et al., 2011; Kumar and Singh, 2018; Mile et al., April 2018; Mile et al., June 2018; Li, 2015; Nabi et al., 2011; Bhandari & Moh, 2016). The WBAN is a collection of wireless sensors placed on the body to collection of the physiological body signs (Arefin et al., 2017). In this Wireless Body Area Network (WBAN), the sensors node can be deployed in two possible ways: implanted and on-body sensors. In the first type of WBAN, sensor nodes are placed inside the body, whereas in the latter, sensors node are placed on the surface of body (Chen et al., 2010). Similarly, there are two ways in which data is transferred between these sensor nodes and coordinator, i.e., Point-to-Point and Multipoint-to-Point (Sipal et al., 2015). In first type, data transfer takes place between any two sensors nodes on the body, whereas in Multipoint-to-Point, data from different sensor nodes are transferred through the same sink, i.e., a coordinator forwards the data to a server located outside the body. Advancements in technology, specifically Nano-technology and routing strategies, have made the field of Wireless Sensor Networking and specifically WBAN very attractive for researchers and developers (ul Huque et al., 2015; AL Rasyid et al., 2015).

The WBANs can be deployed in various applications in the military, sports, medicine, and healthcare, among others (Malik & Singh, 2013; Kumar and Singh, 2018). In health monitoring, sensor nodes can be placed on a patient's body to record the patient data and send it to the coordinator node. For efficient treatment and monitoring, continuous patient monitoring is necessary. In WBAN experiencing delay challenges, this continuous monitoring may not be achievable. Another application is where underwater sensors are deployed underwater environments (Climent et al., 2014). Battlefield networks also are an application of WBAN's. In these battlefields, wireless nodes may be distributed in ad hoc topology. In the application of sensor technology in wildlife management, location and/or movement of wild animals, especially the endangered species, is monitored by implementation of sensor nodes on various parts of the body. In another adaptation of wireless sensor technology, correctional facilities adopt the technology to tracking prisoner's movement. This is achieved by implanting of the sensor nodes on the body such as ankles. The technology also

Author: PhD in Information Technology from Jomo Kenyatta University of Agriculture and Technology, Nairobi, Kenya and is a Scientific Computing and Computer Networks lecturer at the School of Computing and Mathematics in The Co-operative University of Kenya (CUK), Nairobi. e-mail: mileanthony@yahoo.com

assists keeping the security of the prisoners because it alarms when one tries to go beyond the designated safe zone.

Sensor nodes are an essential part of WBAN developers (ul Huque et al., 2015), responsible for data collection and communication with the coordinator for transfer the data. Mobility is a vital aspect of WBAN. When the body on which sensor nodes have been placed or implanted moves, the nodes on the body as well moves hence their coordination with one another changes accordingly. At one moment, nodes are well inside the communication range of one another, and at another moment, there is no connection between two nodes that were previously communicating. The human body shows postural mobility in WBAN, which causes disconnections as discussed by Mile et al. (Mile et al., April 2018; Mile et al., June 2018). In the WBAN mobility situations, instability in the WBAN sensor node connections is experienced due to mobility and distance variation, which causes the channel fading of the sensor node radio frequency.

There are always some performance parameters associated with any network to compute its efficiency. Network delay is a vital parameter in both Wireless Sensor Network (WSN) and WBAN (Jaimes & de Sousa, 2016). In WBAN, we consider three different types of delays as propagation delay, holding or processing delay, and transmission delay. Propagation delay is the delay that the packet takes from the transmitter node to the receiver node as the source and destination nodes are apart. The propagation delay is directly proportional to the distance between the source and destination as distance and inversely proportional to the speed of data. Holding delay or processing delay is the second type of delay in WBAN and it's the processing time of data before transmission it may be due to channel busy. Transmission delay is the third type of delay in WBAN, and it is the time that the node transmits the packet to the destination. It depends on packet size and data rate. When the packet size is large, the transmission delay becomes high but when the packet size is small, transmission delay becomes small. The transmission delay is high if data rate is low and vice versa. Network average delay is some of the propagation delay, proposing delay and transmission delay. Another parameter in determining the performance of a WBAN is energy consumption, which is directly related to battery lifetime. Battery lifetime is an important parameter which defines the efficiency of the network in WBAN. Such network with a longer battery lifetime of sensor nodes with less energy consumption is more efficient compared to a network that utilizes more energy (Prameela & Ponmuthuramalingam, 2016).

In WBAN, due to human body postural mobility, distance variation occurs from time to time between the sensor nodes due to connections drop between sensor nodes. Drops in connections can be short or long, resulting in delays in data transfer, which affects the efficiency of the entire network (Gowtham & Ahila, 2017; Gowtham & Ahila, 2017). Therefore, in WBAN with postural mobility, it is vital to minimize this delay and maximize network lifetime and to create a network that selects the best sink node, hence resulting to a Delay Tolerant Network (DTN). The DTNs represent the class of wireless systems that can support the functionality of a network experiencing repeated and long-term connectivity disconnects. DTN architecture improves performance and extends the range of networks having characteristics as described above. The DTN architectures are used in situations in which there is no conviction about the connection between the sensor nodes, such as underwater sensors and wildlife tracking, field networks.

In this paper, through the proposed postural selection strategy communication model, a WBAN posture selection strategy for determining the sink node locality in different human posture in a DTN is proposed. The existing models show no known adaptation of any sink node selection strategy but rather use statically selected sink nodes. By use of the Omnet++ (Varga, 2015) simulation, the performance of the DTN WBAN can be determined under the postural localities of running and sitting in order to ascertain the optimal postural locality of the sink node. The different postural locality of the sink node is evaluated in each of the mobility scenarios. The results show that the waist locality is the optimal sink position concerning the average delay and power efficiency.

The rest of this paper is organized as follows; section II discusses related work. The proposed work on the WBAN sink node selection strategy and communication model is presented in section III. Section IV presents the algorithm of the proposed postural selection strategy communication model. Section V discusses the simulation of results. Section VI discusses the results. We conclude and discuss future work in section VII.

II. Related Work

A lot of work has been carried out in recent past in the field of DTN, and categorized into two, namely single-copy (Conan et al., 2008; Spyropoulos, Psounis, & Raghavendra 2008a; Leguay et al., 2005; Jain, Fall, & Patra, 2004) and multi-copy (Spyropoulos et al., 2008; Leguay et al., 2007; Lindgren et al., 2004). In single-copy, a single copy of the information is transmitted to the destination node to avoid replication of data packets at destination nodes, which minimizes the replication overhead (Quwaider & Biswas, 2010), which leads to delay minimization but it is necessary that the node is connected in their mobility. On the other hand, the multiple-copy mechanism defines how multiple copies of data packet can reach the destination node through different nodes, which improve the probability of packet delivery ratio (Quwaider, Tanghizadeh & Biswas, 2011) and also increase the overall network delay which case to decrease the network lifetime.

WBAN is a short-range communication network using short transmission range for which different DTN routing mechanisms have been developed (Quwaider & Biswas, 2012). Delivery delays of various routing techniques have been modeled. For the case of single and multi-copy DTN routing, to evaluate the performance of delay in a mobile WBAN by using a working WBAN topology which is developed and use a random posture selection without any specific information of node location for taking locations of on-body movements and applied for data packet routing which is due to the human postural mobility (Quwaider & Biswas, 2012).

The concept of DTN also has been applied by researchers in WSNs to address the problem of intermitted network connections due to work environments and nodes behavior and to achieve power saving in WSNs by the application of Delay Tolerant Network protocol (Li, 2009).

Another research by (Quwaider, Tanghizadeh & Biswas, 2011) presented a stochastic modeling framework for store and forward packet routing in WBAN with postural partitioning. The researchers constructed a prototype for experimentally characterizing and capturing on-body topology disconnections in the presence of ultrashort range radio links, erratic RF attenuation, and the human postural mobility. The concept was that the routing of packet or forwarding would be depended upon the posture of the human body in a WBAN. In their research, a WBANs topology was built for experimentally characterizing the disconnections of link in the presence of a human postural mobility, which then tend to develop a Delay modeling technique for evaluating single-copy on-body DTN routing protocols. This helped reduce the sensor count without losing the packet delay.

Spyropoulos et al. (Spyropoulos, Psounis, & Raghavendra 2008) suggested flooding-based schemes to deal with networks with intermittent connectivity like the case of mobile wireless sensor networks. While flooding-based routing schemes have a high probability of delivery, they waste a lot of energy and suffer from severe contention, which can significantly degrade their performance. They are also plagued by long delays.

Vinaya Kumar (Spyropoulos et al., 2008) proposed an improved multiple copy mechanism by reducing the overhead of flooding-based schemes by introducing a new family of routing scheme that “spray” a few message copies into the network, and then route each copy independently towards the destination. They showed that, if carefully designed, spray routing not only performs significantly fewer transmissions per message.

In conclusion, while the existing single copy mechanisms do not have retransmission overheads, the data packet losses are high due to loss of end to end paths between sensor nodes and sink node leading to less efficiency due to packets loss. The mechanisms may not be ideal for WBAN, which deals with sensitive and critical data in which every single data packet may be lifesaving. On the existing multi-copy mechanisms, the flooding nature of the data packets to increase the chances of data packet delivery leads to energy waste and degraded performance. They also result into packet delays and losses due to link congestion caused by the flooding of traffic. Power saving is an important requirement of WBANs; hence these mechanisms are not ideal. In this paper, a new model was presented. The model uses an approach of dynamic sink node in which while the WBAN nodes are mobile, paths from sensor nodes to sink node are always recreated and the sink node is always reachable. This results into high reliability, high network life-time, and low power consumption of the WBAN.

III. Proposed Network Sink Locality for DTN for Different Postures

This paper presents a postural selection strategy model for determining the sink node locality in different human posture in a DTN. A WBAN topology in Omnet++ is implemented, to demonstrate different sink position in WBAN with different postures. In this section, we describe the WBAN architecture with different postural positions and its applications.

a) Design Considerations: A WBAN Prototype and Variations in Network Topology

In this research, twelve sensor nodes deployed on a human body to construct a WBAN architecture (node zero on the head, node one on the neck, node 2 two on left bicep, node three on right bicep, node four on the waist, node five on the left wrist, node six on right wrist, node seven on left knee, node eight on right knee, node nine on left ankle, node ten on right ankle and node eleven on the chest) as shown in Fig. 1. The CSMA/CA Mac protocol has been used in the research. A WBAN postural mobility can be described as a set of several body posture which exhibit in a human body. In this research, different experiments are performed on every posture to get the optimal position of sink node. Data communication and transmission takes place between sensor nodes and the sink node in every experiment. The responsibility of the sink node is to collect data from every sensor node and send that data to the sink node which transmits to the monitoring server via wireless link. The human body has static and mobile posture according to that, hence the WBAN architecture also changes. Mobile posture has two possibilities as running and walking, in which nodes are mobile, while in case of static posture has three possibilities as standing sitting and lying in which all nodes are stationary. We established and simulated both mobile and static human postures.

In this research, every posture is run for a period interval and the values of delay and energy with different sink node are recorded, which is one of the 12 nodes that communicate to the other nodes. There are certain links, that when connected during certain postures, can lead to changes in the architecture for those postures. Due to the RF attenuation, sometime disconnections occur within a posture. Fig. 1 shows the running body posture in which some parts of human body move continuously. As the leg and hand move continuously so it is the distance between the nodes as it changes time by time in running posture. Due to lot of work in running position, the human body need to send more data, hence the optimal sink selection is crucial.

Walking is also a part of mobile posture, as shown in Fig. 2. In the running posture, maximum mobility was observed on legs and arms, as compared to the other nodes on the body. If we compared the running posture with walking posture, it is found that less mobility was found in the walking as compare to running. It is noted from Fig. 3, that standing posture is a static posture as classified above. Sensor nodes are deployed on the human body to collect data and communicate with the sink node. In static case, the communication between the nodes depends on the distance between the sensor nodes. When we consider that the mobility is zero, then the parameter which effects the sink location is the distance between the sink node and all other nodes. We select the node which has a maximum link with minimum distance as a sink node.

Other possible postures are sitting and lying, as shown in Figures 4 and 5 respectively. Both the sitting and lying are static postures that have no mobility and have a single architecture. In this case, all the performance metrics depend on the node distances. When we consider that the mobility is zeros, then the parameter which effects the sink location is the distance between the sink node and all other the nodes we must select the node which has the maximum link with minimum distance as a sink node.

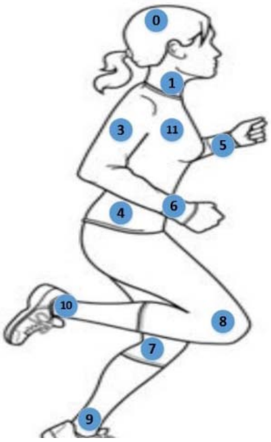


Fig. 1: Running

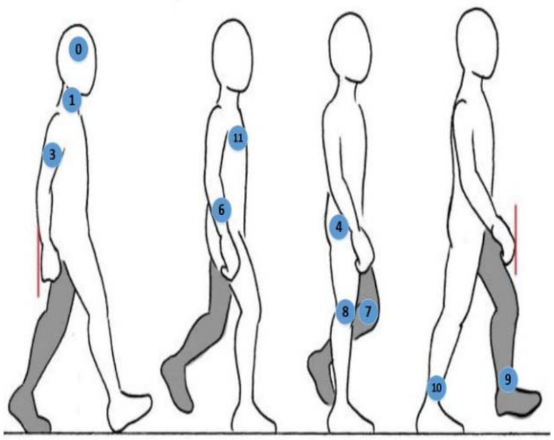


Fig. 2: Walking

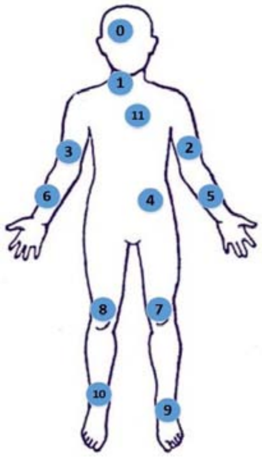


Fig. 3: Standing

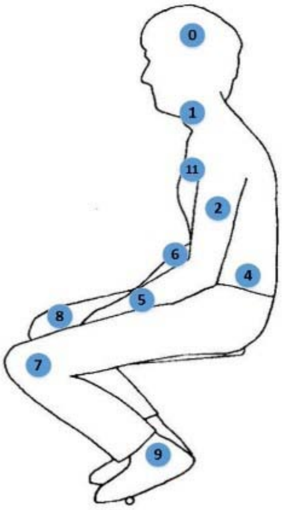


Fig. 4: Sitting

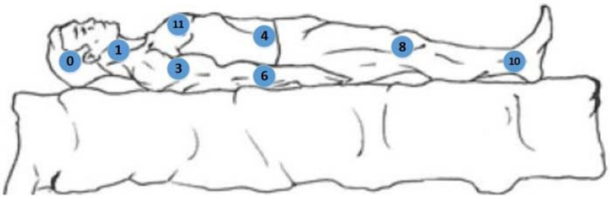


Fig. 5: Lying down

b) MoBAN Posture Selection Strategy

The human body can be in five different postures, which are broadly categorized in two ways as mobile postures and static or stationary postures. Fig. 6 shows the MoBAN posture selection scheme and its description. We consider two types of postures in our scheme, namely Mobile postures and Static postures.

In both case, whether the posture is mobile or static, the selector needs to find whether it is a mobile or a static posture in first stage. If the posture is mobile, then the target location and speed of nodes is specified by the coordinator. The node keeps moving until the destination reached.

In the static posture case, the simulation time is fixed. After time selection, the posture is selected. Once the simulation time is complete, a control is sent to the posture selector if all postures are not executed. The posture is executed until all postures are selected and then simulation ends.

c) Network Sink Locality for DTN for different Postures

In a WBAN environment, several sensors are placed on a human body for the collection of data regarding a medical condition or body movements. We created such a WBAN in Omnet++ environment composed of 12 nodes strategically placed on different body parts, as can be seen in Figures (1, 2, 3, 4, and 5). The coordinator node controls the mobility of nodes. It also performs the duty of synchronizing the movements of sensor nodes. Coordinator plays an equivalent role as the human brain in real life scenario, i.e. specifying to move, setting target position, setting the speed to move towards target position, etc. In this paper, we find the most suitable location of the sink node (one of the 12 nodes) such that minimum network resources are utilized, and a more enhanced performance network can be realized.

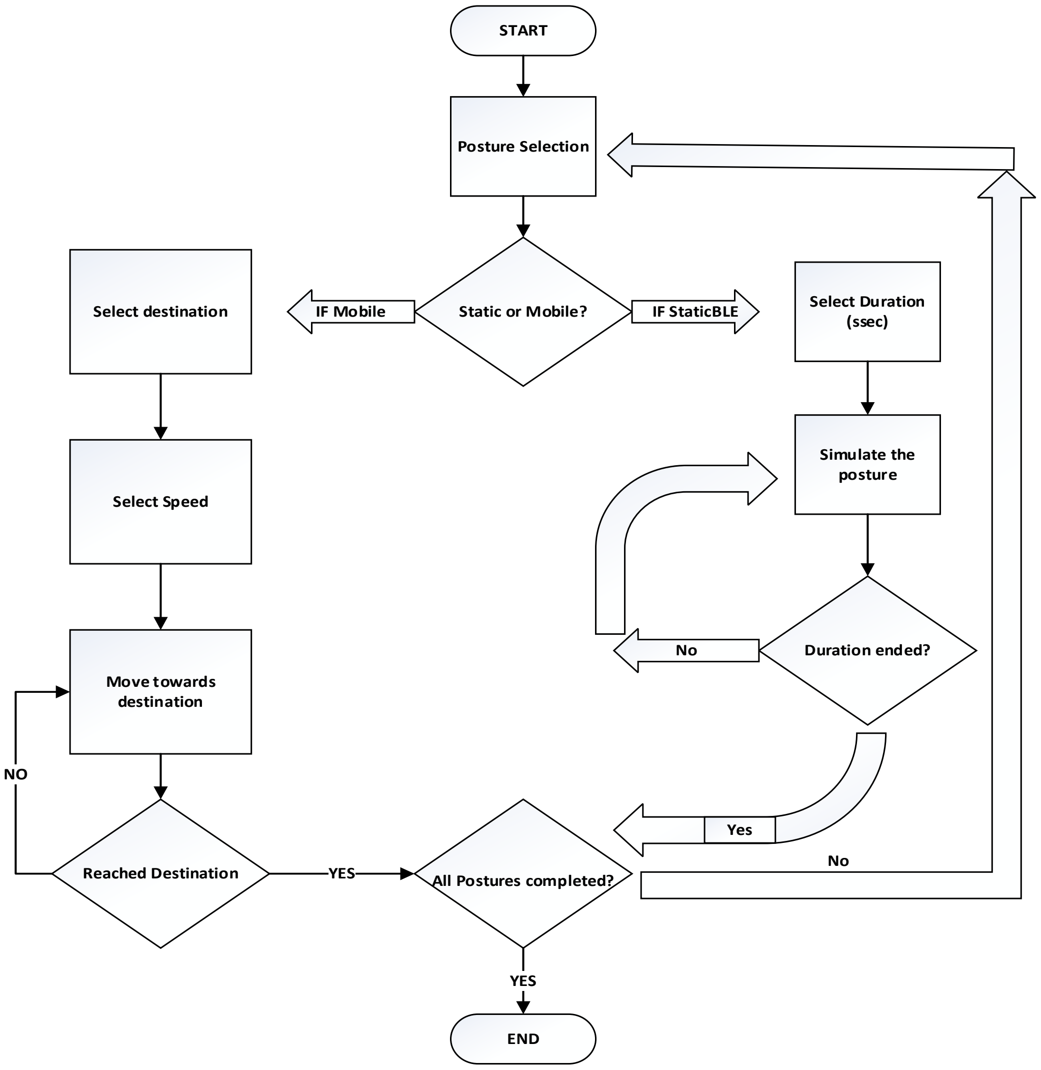


Fig. 6: MOBAN Posture Selection Strategy

The selection of suitable sink location can be critical for the performance of the network, but this is not a straight forward decision. As we select five different postures, three of them, as sitting, lying and standing are considered as stationary postures, while walking and running postures are considered as mobile postures. Greater mobility indicates high utilization of resources, i.e., battery, time, etc. In WBAN, due to postural mobility, there can be long lasting delays between different sensors. Therefore, while making a suitable selection of sink position, different factors need to be considered.

This research simulates a network for all the nodes to act as a sink and compared the performance of a network. All the sensor nodes transmit the data packet to a sink node. The sink node also sends packets to all other nodes after a specific time period to keep them alive and active.

The algorithm I describe the general flow of the research scenario. The coordinator is a component in our scenario which handles the mobility and synchronization of sensor nodes. The coordinator specifies the target position to each node and node moves to the specified location. When nodes reach their targeted positions, then the selection of the transmission node is done. Out of 12 nodes in our scenario, only one node sends the data packet at a time. The selected transmission node checks the medium availability. If it finds the medium free, it transmits its packet to the destination node. Otherwise, a back off counter is incremented. It then checks whether time allotted for transmission (transmission counter=0.021 seconds) to a specific node expires or not. If the transmission counter expires, then another node is selected as the transmission node. Otherwise, the selected node waits for a specific interval time then checks medium availability. Similarly, a random node is selected among receiver nodes to acknowledge the reception of packet. The selected node checks the availability of medium, and in case of free medium, it sends the acknowledgement. If the medium is unavailable, the backoff counter of the respective node is incremented.

Then, it checks whether time allotted for acknowledgment (transmission counter = 0.021 seconds) expires or not. If transmission counter expires, another node for acknowledging the transmission node is selected. Otherwise the selected node waits for a specific counter before it checks medium availability again. After that, it checks the simulation timer expiry. If expired, the simulation is ended. Otherwise, control is passed to the coordinator which specifies the new target position for the nodes and the whole process is repeated until the simulation timer (defined before simulation) gets expired.

IV. Algorithm of the Proposed Postural Selection Strategy Communication Model

a) The Postural Selection Strategy Communication Model

The proposed communication model is presented in the algorithm below. It shows the flow steps from the time the coordinator position is specified until the end of simulation time.

Start simulation time specify the coordinator position Nodes move in a specific location Select transmitting node if medium available for node Transmit data wait for acknowledgement if receiver node find channel available send acknowledgement if simulation timer expires end else Go back and specify the coordinator position Repeat process else increment backoff counter if simulation timer expires Receiver node checks channel availability else wait for a specific time Receiver node checks channel availability wait for medium free else increment backoff counter if transmission counter expire select transmitting node check channel availability else wait for a specific time check channel availability End.

V. Simulation Results

This research has implemented basic postures of a human body as static posture (sitting) and mobile posture (running) in OMNET++ (v.4.6) and executed a sequence of experiments to find the best location of the sink node. Data packets from sensor nodes are transferred to the destination node.

In order to avoid collisions, CSMA/CA MAC protocol is implemented so that only one node utilizes the communication channel at a time. During simulation, all nodes in a network forwards data to current sink node which transmits the data to the coordinator.

In this paper, the network delay is minimized. The network delay depends on the location of sink node. It is affected by the distance between the sensor nodes and the sink node. Energy Consumptions is another performance metric which affect the network lifetime. List of parameters used in this scenario is shown in Table 1.

Table 1: Simulation Parameters

Parameter Name	Value
pMax	110.11mW
Carrier Frequency	2.412x 10^9Hz
Alpha	3.0
Saturation	-110dBm
Time Tx to Rx	0.00012s
Time Tx to sleep	0.000032s
Queue Length	5
Header Length	24bit
Max Tx Attempts	14
Bitrate	15360bps
Tx Power	110.11mW
Sleep Current	10
Tx Current	5000
Rx Current	25

a) Average Delay

Delay is an important parameter describing the overall performance of the network. Therefore, we are interested in finding a sink node position which minimized the overall network delay. In WBAN, the distance between the nodes and the sink node is an important factor which determine the delay of the network. The distance between the sensor nodes and sink node change regularly due to postural mobility. Distance between a node and sink node is directly proportional to the delay. Average delay not only depend on the distance of the nodes, but also depends on the channel accessibility, i.e., less processing delay. Similarly, WBAN mobility also plays a vital role in network delay. As a mobile node changes position in the network, it also informs the rest of the nodes about its new position. Thus, as mobility increases, these positions notification packets also increases increasing the congestion and average delay of the network.

Running: The simulation was run for all the nodes as sink nodes. Some of the best choices for sink nodes (head, waist, chest, wrist, and ankle) are given in Fig. 7. The starting point of the average delay curve for every node as sink depends upon the time at which the respective node was involved in the network. It is evident from Fig. 8 that when the node the ankle was selected as the sink node due to the high mobility of ankle node the delay of network increase, the node at head compare to ankle is less mobile, so it shows a small increment in delay than ankle node while when select he node on the waist as a sink its shows optimal performance in mobile network delay due to less mobility and nearest to all other nodes. Thus, the node at waist proves to be the optimal option to be considered as sink node running posture.

Sitting: The simulation was run for all the nodes as sink nodes. Some of the best choices considered as sink nodes (head, waist, chest, wrist, and ankle) are given in Fig. 8. The starting point for the average delay curve for every node as sink depends upon the time at which the respective node was involved in the network. Sitting posture is a static network, therefore, it does not depend on the mobility of nodes, but it depends on the distance of the nodes to the sink node as shown in Fig. 8. When we select node at the head as a sink node, due to maximum distance from other nodes it shows maximum delay when compare to the ankle and the waist node positions. When the node on waist was selected as the sink, its shows optimal performance in sitting posture because the waist position is nearest to all other nodes. Thus, node at waist proves to be the optimal option to be considered as sink node in sitting posture.

Overall Network: The simulation was run for all the nodes as sink nodes, but some of the best choices to be considered as sink nodes (head, waist, chest, wrist, and ankle) are given in Fig. 9. The starting point of the average delay curve for every node as sink depended on the time at which the respective node was involved in the network. As in overall network, we consider both the mobile posture as well as static posture. As shown in Fig. 9, the ankle position as sink node led to high delay. This can be attributed to the high mobility nature of the legs. The head position when compared to ankle position of the node, the head being less mobile than the ankle, showed slightly better delay performance than the ankle. The node on waist as a sink showed the optimal performance in overall network delay due to less mobility and nearest to all other nodes. Thus, node at waist proves to be the optimal option to be considered as sink node.

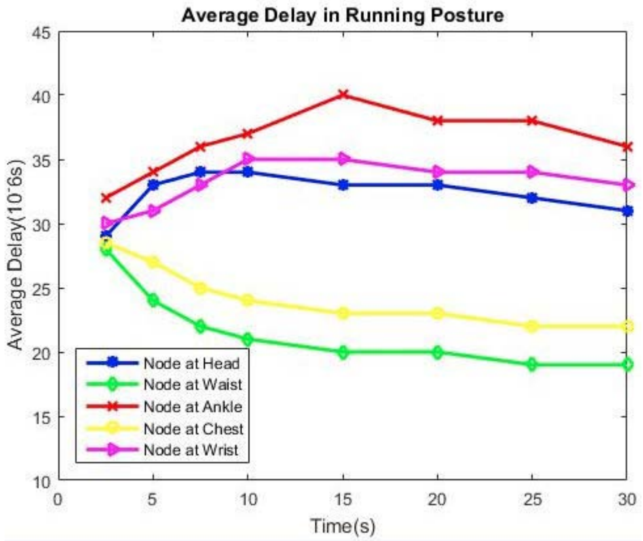


Fig. 7: Lying Average Delay in Running Posture Selection

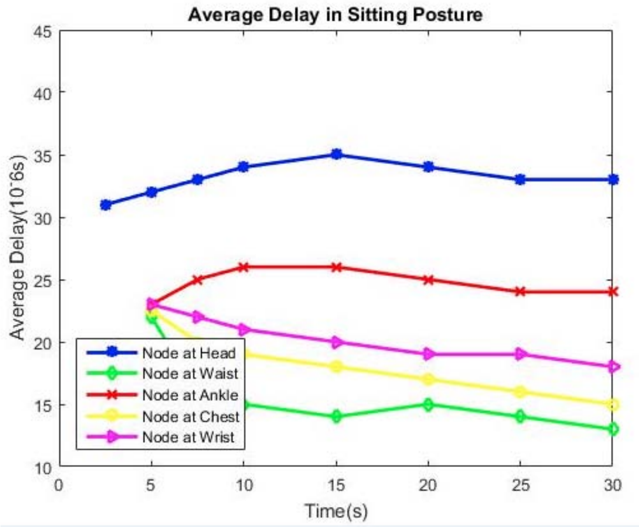


Fig. 8: Average Delay in Sitting Posture Selection

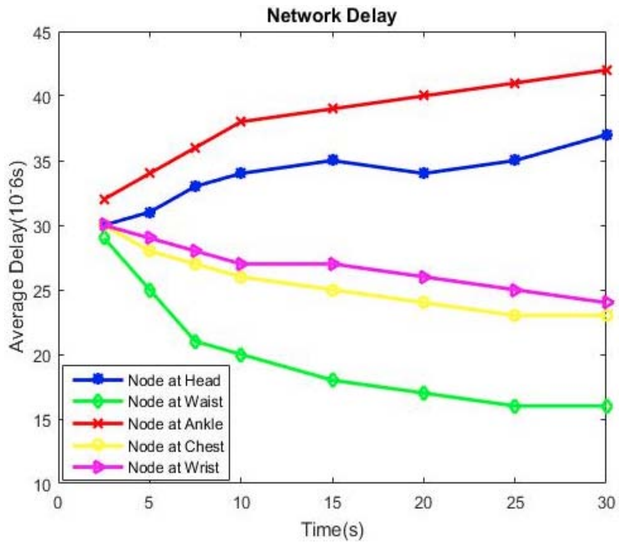


Fig. 9: Average Delay in Overall Network

b) Energy Consumption in different Posture

Battery Battery lifetime is a crucial parameter in WSNs and especially in WBAN's because some of the sensor nodes are deployed inside the body, which means they are not easily and frequently removed out. This means that the battery life is a critical feature of the sensor node. Therefore, there is need to minimize the energy consumption of sensor nodes to improve the battery lifetime and energy consumption. The battery lifetime and energy consumption are directly depended on both the node distance to the destination node and the number of retransmission. In our scheme, all the node communicates with the sink node so the distance between the sink node the other maximum node should be shorter.

In this research, the simulation was run on two different postures only, running as the mobile posture and sitting as the stationary posture. In the sitting posture, all the nodes were considered as stationary for comparison of different sink location as the head node, the waist node and the ankle node.

Running: The simulation was run for all the nodes as sink nodes with head, waist, chest, wrist, and ankle positions being considered. The results are shown in Fig. 10. In this posture, nodes move continuously, hence increasing the energy consumption of the sink. From Fig. 10 it is shown that energy consumption of nodes at ankle is highest than energy consumption at node deployed on the head and the waist due to the high mobility of ankle in running posture. Energy consumption also depend on the distance between the sink and the other node, the node which is nearest to the other node has least energy consumption as shown in Fig. 10 the energy consumption at the waist node is least than the other two so the node at the waist is best choice for a sink in running posture according to energy consumption.

Sitting: The simulation was run for all the nodes as sink nodes. These are the head, waist, ankle, chest and the wrist as shown in Fig. 11. Like in the Sitting posture, there is no mobility involved, the energy difference is based on the postural locality of sink node from other nodes and coordinator. The greater the distance between the sink node from other nodes and coordinator, the greater is the energy consumption of that specific node. As node at the waist was located at the center of body, its distance from the other nodes was smaller as compared to other nodes in Fig. 11. That is why energy consumption of node at waist is smaller than other nodes in Fig. 11. Therefore, we conclude that the node at waist is the ultimate choice of sink node in Sitting Posture in relation to energy consumption.

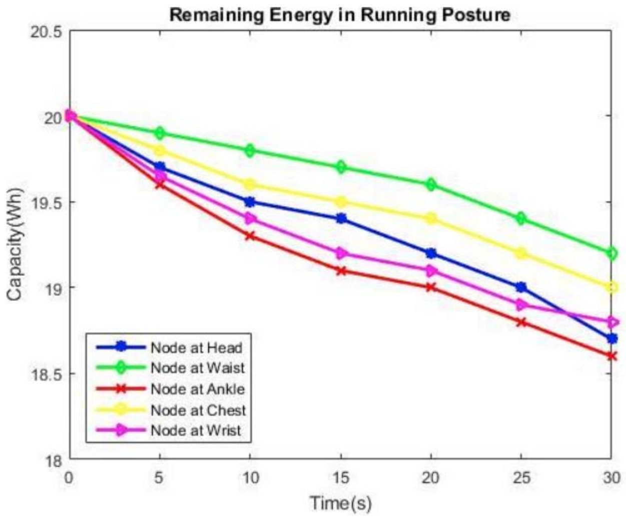


Fig. 10: Average Energy Consumption in running posture

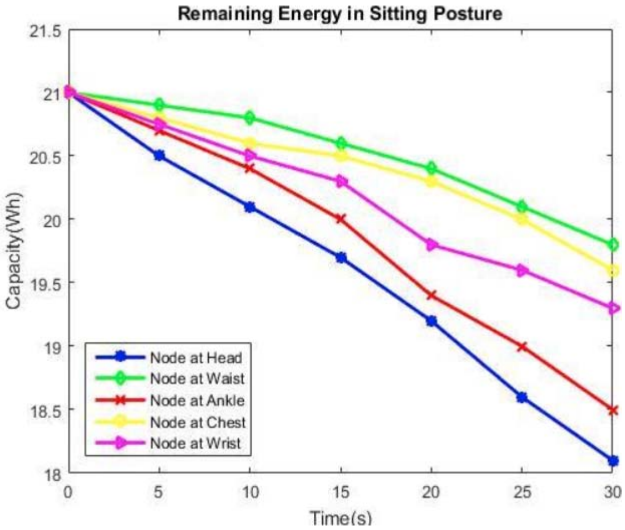


Fig. 11: Energy Consumption in Sitting Posture

VI. Discussion of Results

From the review in the introduction, it was determined that the selection of suitable sink position can be critical for the performance of a DTN WBAN and that this selection is not a straight forward decision. In this study, a posture selection strategy has been proposed, as outlined in Fig. 6 and the pseudocode. The performance evaluation shows that the average delay has been minimized in the proposed sink locality under the proposed selection strategy under the running and sitting postures. The performance of the different sink node under the various localities, such as the head, ankle, and the waist location in each postural scenario showed that waist location as the best in performance. The delay was recorded to increase as the node moves away from the sink node. The energy consumption showed that the waist position sink node locality has the least energy consumption of the three localities evaluated. This can be related to the fact that nodes far away from waist node have higher mobility hence the reason for high energy consumption.

VII. Conclusion and Future Work

The Network lifetime improvement and delay minimization is a key research issue in WBAN. Improper sink selection is one of the main causes of data loss in WBAN due to different posture and WBAN mobility. Various parameters need be observed while selecting the optimal sink position for all the postures. The node with the least mobility and at proximity to the center of body is consider as a sink node. This research proposed a WBAN posture selection strategy which when applied to WBAN with mobility, the best optimal sink node locality is selected. This leads to improved WBAN performance in terms of average WBAN delay and energy consumption. In the evaluation of the sink node selection strategy, it is observed that waist sink node locality is the best optimal position as it gives the minimum average delay and energy consumption. In the future, more work should explore mechanisms for dynamic sink node locality to ensure optimal WBAN efficiency.

References Références Referencias

1. Arefin, M., Ali, M. and Haque, A. (2017) Wireless Body Area Network: An Overview and Various Applications. Journal of Computer and Communications, 5, 53-64. doi: 10.4236/jcc.2017.57006
2. Bhandari, S., & Moh, S. (2016). A priority-based adaptive MAC protocol for wireless body area networks. Sensors, 16(3), 401.
3. Chen, W., Hu, J., Bouwstra, S., Oetomo, S. B., & Feijs, L. (2011). Sensor integration for perinatology research. International Journal of Sensor Networks, 9(1), 38-49.
4. Chen, K. Y., & DAVID R BASSETT, J. R. (2005). The technology of accelerometry-based activity monitors: current and future. Medicine & Science in Sports & Exercise, 37(11), S490-S500.
5. Climent, S., Sanchez, A., Capella, J. V., Meratnia, N., & Serrano, J. J. (2014). Underwater acoustic wireless sensor networks: advances and future trends in physical, MAC and routing layers. Sensors, 14(1), 795-833.
6. Conan, V., Leguay, J., & Friedman, T. (2008). Fixed point opportunistic routing in delay tolerant networks. IEEE Journal on Selected Areas in Communications, 26(5).
7. Darkins, A., Ryan, P., Kobb, R., Foster, L., Edmonson, E., Wakefield, B., & Lancaster, A. E. (2008). Care Coordination/Home Telehealth: the systematic implementation of health informatics, home telehealth, and disease management to support the care of veteran patients with chronic conditions. Telemedicine and e-Health, 14(10), 1118-1126.
8. Gowtham, M., & Ahila, S. S. (2017). Privacy enhanced data communication protocol for wireless body area network. In Advanced Computing and Communication Systems (ICACCS), 2017 4th International Conference on (pp. 1-5). IEEE.
9. Jaimes, A. F., & de Sousa, F. R. (2016). A taxonomy for learning, teaching, and assessing wireless body area networks. In Circuits & Systems (LASCAS), 2016 IEEE 7th Latin American Symposium on (pp. 179-182). IEEE.
10. Jain, S., Fall, K., & Patra, R. (2004). Routing in a delay tolerant network (Vol. 34, No. 4, pp. 145-158). ACM.
11. Kumar, A., & Singh, P. (2018). Energy Efficient Transmission Approach for WBAN Based on Threshold distance. Energy, 5(02).
12. Leguay, J., Friedman, T., & Conan, V. (2007). Evaluating MobySpace-based routing strategies in delay-tolerant networks. Wireless communications and mobile computing, 7(10), 1171-1182.
13. Leguay, J., Friedman, T., & Conan, V. (2005, August). DTN routing in a mobility pattern space. In Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking (pp. 276-283). ACM.
14. Li, L. (2009). Modeling and Analysis on a DTN Based Wireless Sensor Network Topology Control. International Journal of Computer Network and Information Security, 1(1), 32.
15. Li, C., Yuan, X., Yang, L., & Song, Y. (2015). A hybrid lifetime extended directional approach for WBANs. Sensors, 15(11), 28005-28030.
16. Lindgren, A., Doria, A., & Schelen, O. (2004). Probabilistic routing in intermittently connected networks. In Service assurance with partial and intermittent resources (pp. 239-254). Springer, Berlin, Heidelberg.
17. Lv, Z., Xia, F., Wu, G., Yao, L., & Chen, Z. (2010, December). iCare: a mobile health monitoring system for the elderly. In Green Computing and Communications (GreenCom), 2010 IEEE/ACM Int'l Conference on & Int'l Conference on Cyber, Physical and Social Computing (CPSCom) (pp. 699-705). IEEE.
18. Malik, B., & Singh, V. R. (2013). A survey of research in WBAN for biomedical and scientific applications. Health and Technology, 3(3), 227-235.
19. Mile, A., Okeyo, G., & Kibe, A. (2018, June). Adaptive Cluster Head Selection Scheme for High Mobility Based IEEE 802.15. 6 Wireless Body Area Networks. Journal of Sensor Technology, 8(02), 35.
20. Mile, A., Okeyo, G., & Kibe, A. (2018, April). Hybrid IEEE 802.15. 6 Wireless Body Area Networks Interference Mitigation Model for High Mobility Interference Scenarios. Wireless Engineering and Technology, 9(02), 34.
21. Nabi, M., Geilen, M., & Basten, T. (2011, March). MoBAN: A configurable mobility model for wireless body area networks. In Proceedings of the 4th international ICST conference on simulation tools and techniques (pp. 168-177).
22. Prameela, S., & Ponmuthuramalingam, P. (2016). A robust energy efficient and secure data dissemination protocol for wireless body area networks. In Advances in Computer Applications (ICACA), IEEE International Conference on (pp. 131-134). IEEE.
23. Quwaider, M., & Biswas, S. (2008). Body posture identification using hidden Markov model with a wearable sensor network. In Proceedings of the ICST 3rd international conference on Body area networks (p. 19). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

24. Quwaider, M., & Biswas, S. (2010). DTN routing in body sensor networks with dynamic postural partitioning. Ad hoc networks, 8(8), 824-841.
25. Quwaider, M., Taghizadeh, M., & Biswas, S. (2011). Modeling on-body dtn packet routing delay in the presence of postural disconnections. EURASIP journal on wireless communications and networking, 2011, 3.
26. Sipal, V., Gaetano, D., McEvoy, P., & Ammann, M. J. (2015). Impact of hub location on the performance of wireless body area networks for fitness applications. IEEE Antennas and Wireless Propagation Letters, 14, 1522-1525.
27. Spyropoulos, T., Psounis, K., & Raghavendra, C. S. (2008). Efficient routing in intermittently connected mobile networks: The multiple-copy case. IEEE/ACM transactions on networking, 16(1), 77-90.
28. Spyropoulos, T., Psounis, K., & Raghavendra, C. S. (2008b). Efficient routing in intermittently connected mobile networks: The single-copy case. IEEE/ACM transactions on networking, 16(1), 63-76.
29. ul Huque, M. T. I., Munasinghe, K. S., & Jamalipour, A. (2015). Body node coordinator placement algorithms for wireless body area networks. IEEE internet of things journal, 2(1), 94-102.
30. Varga, A. (2001, June). Discrete event simulation system. In Proc. of the European Simulation Multiconference (ESM'2001).
31. Yi, Z., Shan, Z., Wang, J., Li, J., Cheng, C., Haoting, X., ... & Xiao, S. (2016). Ubiquitous healthcare system using emergency strategy based on wireless body area system. In Computer Science and Network Technology (ICCSNT), 2016 5th International Conference on (pp. 117-120). IEEE.

This page is intentionally left blank

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 20 Issue 1 Version 1.0 Year 2020
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 2249-4596 & Print ISSN: 0975-5861

Introducing Connected Dominating Set as Selection Feature of Cluster Heads in Hierarchical Protocols of Wireless Sensor Networks

By Chiranjib Patra

Abstract- It has been found that almost all routing protocols do suffer from efficiency of its operation regarding data transfer from one point to another. To overcome this process algorithm regarding the choice of nodes as cluster heads has to be done with utmost care. Failing of this leads to unnecessary dissipation of energy such as generating excess 'Hello' messages and less useful data transfer. In this communication we show that the introduction of connected dominating set as one of the metric regarding the choice of cluster head leads to better data transfer and energy consumption. Moreover we implemented this concept in LEACH protocol and found acceptable improvement in the performance parameters of the protocol.

Keywords: hierarchical protocol, LEACH, connected dominating sets, clustering.

GJCST-E Classification: C.2.m

Introducing Connected Dominating Set as Selection Feature of Cluster Heads in Hierarchical Protocols of Wireless Sensor Networks

Chiranjib Patra

Abstract- It has been found that almost all routing protocols do suffer from efficiency of its operation regarding data transfer from one point to another. To overcome this process algorithm regarding the choice of nodes as cluster heads has to be done with utmost care. Failing of this leads to unnecessary dissipation of energy such as generating excess 'Hello' messages and less useful data transfer. In this communication we show that the introduction of connected dominating set as one of the metric regarding the choice of cluster head leads to better data transfer and energy consumption. Moreover we implemented this concept in LEACH protocol and found acceptable improvement in the performance parameters of the protocol.

Keywords: hierarchical protocol, LEACH, connected dominating sets, clustering.

I. Introduction

Wireless Sensor Network [3, 4] (WSN) consists of sensor nodes dispersed randomly over the area under consideration. These nodes communicate among each other by multi hop are single hop depending upon the energy of the nodes. The Base Station (BS) is a node which is powered externally does the job of data aggregation to the IoT channel or any other interpreting software as desired. The BS can also communicate the information to each node in the same way. Because of the harsh environmental condition these sensor nodes once deployed can have limited chances of battery replenishment. Hence gathering sensed data in an energy efficient manner is time critical for the sensor network over a long period of time [5]. Hence limiting the energy dissipation and stretching the network lifetime is one of the most important factors in WSN [4, 5].

This paper focuses on cluster based data transmission schemes as it helps to prolong the network lifetime of WSNs. In this technique nodes are elected as CHs from a subset of nodes which are eligible to become CH on the basis of energy consideration and belong to connected dominating set as additional requirement. The remaining nodes act as non-CH to save its own energy, and transmits its data to the elected CH. CH performs data aggregation on the data received from its member nodes. This method of data transmission is energy efficient as the energy required for communication is high compared to the energy required for computation [6], [7]. The CH should be on rotational basis and so are the cluster members to avoid early death of CHs. This is required because many actions are performed by each elected CH, including cluster head announcement through hello packets, an announcement of data transmission schedule to the member nodes, reception of data from member nodes, data aggregation, and transmission of collected data to base station.

Clustering algorithms are divided into two types as Distributed Clustering and Centralized Clustering. Distributed clustering method is again split into four sub types based on the cluster formation idea and parameters used for CH election as Identity based, Neighborhood information based, Probabilistic, and Iterative respectively. Linked Cluster Algorithm [8] belongs to Identity based clustering technique that takes unique node identifiers as primary key to select the cluster heads. In another improvement Linked Cluster Algorithm also helps to eliminate chances of multiple cluster head selection [8]. There are a good number of protocols devised using Neighborhood Information based approach. Highest Connectivity Cluster Algorithm (HCCA) [8], is based on choosing a sensor node as cluster head which has greatest number of neighbors at 1-hop distance with clock synchronization as an additional requirement. Max-Min D- Cluster Algorithm [9], selects cluster head in such a way that no neighbors are at d-hop distance away from it and thus givingbetter load balancing without any clock synchronization requirement. Weighted Clustering Algorithm (WCA) [10], functions on the basis of the principle of non- periodic initialization of itself only when topology reconfiguration has become unavoidable due to a particular node dissipating energy. This loss of energy leads to losing connectivity with its cluster head which in turn tries to balance the combination of several required parameters

Author: Department of Information Technology, Calcutta Institute of Engineering and Management kolkata, India.
e-mail: chiranjibpatra@gmail.com

called 'combined weight'. Grid-clustering routing Protocol (GROUP) [11], uses multiple sinks among which one of them is considered as 'primary sink'. This being responsible for dynamically selecting cluster heads which forms a grid-like structure. Probabilistic Approaches for clustering in WSN relies upon a prior assigned probability values for sensor nodes. Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol in [12] provides a rational use of energy by random rotation of cluster heads on the basis of energy. This process meanwhile assures uniform load balancing in one-hop sensor networks. Hybrid Energy Efficient Distributed Clustering (HEED) proposes a way in which the remaining energy of sensor nodes and intra-cluster data exchange costs in the competitive way of selecting the cluster heads in multi hop sensor networks [14, 15]. Energy Efficient Clustering Scheme (EECS) proposes dynamic, and localized hierarchy based process for selection of cluster heads based on the basis of energy of sensor nodes providing lower message overhead and uniform distribution of cluster heads [14]. Two-Level LEACH (TL-LEACH) is proposed in [13], which is an extension to LEACH, proposing primary and secondary tier of cluster head selection to minimize energy utilization.

Iterative clustering protocols that is be mentioned here are: DCA [16], SPAN [17], and ACE [18]. Distributed Clustering Algorithm (DCA) protocol uses time delayed notification technique for any sensor before selecting the cluster head and thus giving a chance for other hierarchical preference conditions neighbor sensor nodes to become the cluster heads. SPAN is a randomized cluster head selection process with spatial decision making process which is based on number of sensor nodes being benefited and its own energy levels for a sensor node that is likely to become cluster head. Algorithm for Cluster Establishment is one the sought protocol primarily used for energy saving, with two distinct phases of cluster head selection: a randomized new cluster ‘spawning phase’ and ‘migration phase’ for existing clusters to achieve highly uniform non-overlapping cluster formation. But iterative clustering suffers from too much dependency on neighbors and thus the network diameter.

Our communication is divided into six sections the first section is the brief introduction to the connected dominating set algorithms and clustering process in sensor network, second section deals with the brief review of the protocols on which will be used to modify hierarchical protocol , the third section gives the list of assumptions and the theoretical framework of how the connected dominating set be integrated with LEACH , the fourth section deals with simulator specifics built on MATLAB , the fifth section deals with results and discussions on the data generated by the simulator, sixth section concludes the paper with conclusions and future work.

II. Brief Review on the Protocols used

LEACH: LEACH is one of the popular clustering routing protocols for wireless sensor networks (WSNs) to increase the lifespan of network. It is a self-organizing protocol that balances the energy load equally among all the sensors of the network. In LEACH, nodes elect cluster head (CH) and one node from that cluster acts as its CH. LEACH chooses high energy sensor node as CH but after a round has been performed, it rotates CH among all nodes of the network so that the energy of a single node is not drained completely. Thus LEACH reduces energy dissipation and increases network lifetime. For each round, sensors elect themselves as CH with certain probability determined by a function. The status of these CHs is broadcasted within the network with the help of Hello messages. Each sensor node selects its CH by choosing the one which requires minimum communication energy by evaluating the Euclidian distance between the nodes. Then the CH uses TDMA for the nodes to transmit data. In this way, nodes transmit data to the CH in their time slot and are in sleep condition for the rest of the time. So, the energy consumption of non-CH sensor node is minimized.

When the CH receives all the data from non-CH sensor node within its cluster, it collects that data and sends it to BS. In this way, energy dissipation of the whole network is reduced. A CH uses more energy as compared to member nodes. To overcome this issue, LEACH has a fixed number of CH and a CH is self-elected at every round. For a node to become CH depends on energy of that node. So, node with higher remaining energy acts as CH for that round.

Connected Dominating Set algorithm: This algorithm is especially attractive in ad hoc networking in the area of mobile communication and sensor networks. This algorithm actually is very easy to compute and has the complexity of O(n). For example, to connect a backbone nodes in ad hoc sensor networks to perform efficient routing and broadcasting. A Connected Dominating Set (CDS) can be used as a backbone. Backbones improves the routing procedure and reduces the communication overhead, decreases the overall energy consumption, increases the bandwidth efficiency, and, at last, increases network lifetime in a WSN. The nodes in CDS are called dominator (backbone node) other nodes are called dominatee (non-backbone node). This process is easy to adapt in case of WSN.

Rai et al. [1] proposed an algorithm for finding Minimum Connected Dominating Set (MCDS) which are connected through Steiner tree. The approximation algorithm includes of three stages.

- The DS is determined through recognizing the maximum degree of those nodes to discover the highest cover nodes.

- The connectivity of the nodes in the DS is verified through a Steiner tree.
- At last, this tree prunes to form the MCDS.

Xie et al. [3] called their algorithm as Connected Dominating Set-Hierarchical Graph (CDS-HG). It is a approximate distributed MCDS algorithm. The authors proved that this algorithm generates smaller CDS as compared with other existing algorithms. Their algorithm operates of two phases.

- At first, in the first phase, (Essential Node Determination) is used. According to this step, a set of dominators select for each level so that all nodes in the next upper level are dominated by these dominators. A greedy algorithm is used to select the dominators for creating a small initial DS.
- In the second phase, is used to remove the redundant dominators. This process repeated from the lowest level to the highest level of the graph. Thus the greedy strategy used in previous step provides the result as connected DS.

III. Assumptions and Theoritical Background

Any protocol that guarantees certain properties has to make certain valid assumptions. However if the assumptions are explicit then it becomes the responsibility of the developer to satisfy the assumptions. These assumptions are mostly network latency and bandwidth, processing time, failures, and so on.

So in the premise of LEACH [19] the following are the assumptions:

1. The sensors in the wireless sensor network are distributed randomly in a two dimensional space.
2. The communication environment is contention- and error-free; hence, sensors do not have to retransmit any data.
3. Data exchanged between two communicating sensors not within each others' radio range is forwarded by other sensors.
4. The radio model considered is similar to LEACH.
5. Randomized, adaptive and self-configuring cluster forming.
6. Localized control over data transfers.

In the premise of CDS construction Li et al. [2] algorithm for constructing CDS is used. It is called as Approximation Two Independent Sets based Algorithm (ATISA). The ATISA has three stages:

- Constructing a connected set (CS)
- Constructing a Connected Dominating Set
- Pruning the redundant dominators of CDS.

ATISA constructs the CDS with the smallest size, compared with some well-known CDS construction algorithms. The message complexity of this algorithm is O(n).

Keeping the view of message complexity part the choice of using Li et al algorithm is used.

In LEACH the distributive algorithm works on the basis of selecting clusters which have higher energy than threshold value. But the logic of the choice is entirely based on energy levels but the connectivity part is not taken care of. As the result not all nodes in the cluster may be able to send the data to the cluster head. Thus by considering the connected dominating set the cluster head positions will be in a perfect position to receive the data.

So by using the concept of connected dominating as an additional requirement other than energy requirements is incorporated in LEACH algorithm to get improved performance results.

Below depicts the hybrid CDS-LEACH flow chart for selecting heads and their operation in tandem.

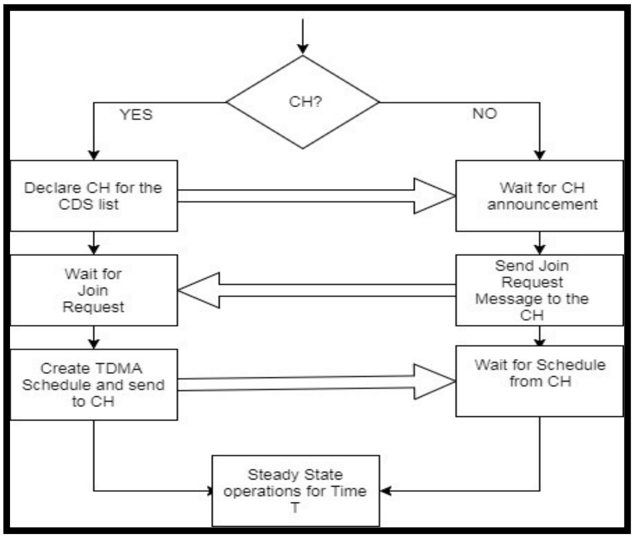

CH?
YES
NO
Declare CH for the CDS list
Wait for CH announcement
Wait for Join Request
Send Join Request Message to the CH
Create TDMA Schedule and send to CH
Wait for Schedule from CH
Steady State operations for Time T

Figure 1: CDS-LEACH cluster head selection algorithm

IV. Simulator Specifics

The simulation is based on simulating the LEACH and CDS-LEACH algorithms in MATLAB considering the following parameters as given in the table.

Table 1: The simulation parameters

Sr. No.	Description	Value
1	Radio electronic energy	50nJ
2	Bitrate	1mbps
3	Antenna height from the ground	1.5 m
4	Antenna Gain factor	1
5	Signal wavelength	0.325m
6	Radio Amplifier energy	10pJ/bit/m2
7	Network size	100mX100m
8	Radio propagation speed	3X10^8
9	Base Station Coordinates	(0,0)
10	Optimum Cluster Size [19]	C*√N*M/d^2

V. Results and Discussions

The Simulator as described is used with two kind of protocols

1. LEACH
2. CDS-LEACH

When these protocols are run according to the standard algorithm the following are the output regarding the cluster formation and cluster heads.

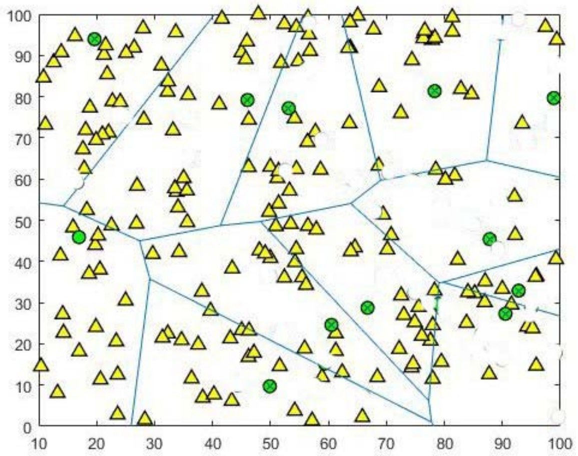


Figure 2: The LEACH protocol implementation for 250 nodes network. The cluster shapes are represented in voronoi cells and cluster heads in green circles for the last round. And the yellow triangles are the normal nodes

The node distribution over the network area is random and the base station is at the origin bottom left not shown in the picture.

Similarly for CDS-LEACH the simulation was carried out and the screen short of the last round of the simulation is as depicted in the figure below.

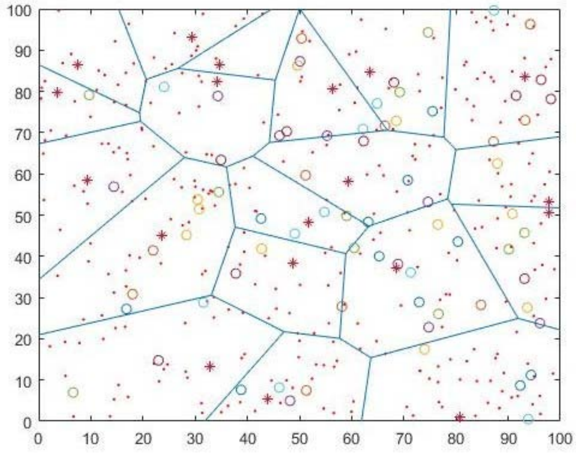


Figure 3: The screen shot for the last round of the execution of CDS-LEACH protocol for 400 nodes. The asterisk nodes were the cluster head nodes for the last round .Here the base station is in the bottom left not shown in the figure. The circles are positions of CDS fulfilled nodes

The performance comparison between the LEACH and CDS- LEACH for dead nodes versus round, average energy spent versus round and data transfer versus round has been shown below to describe the performance metrics.

Below is the representation of 250 node simulation for LEACH and CDS LEACH protocol.

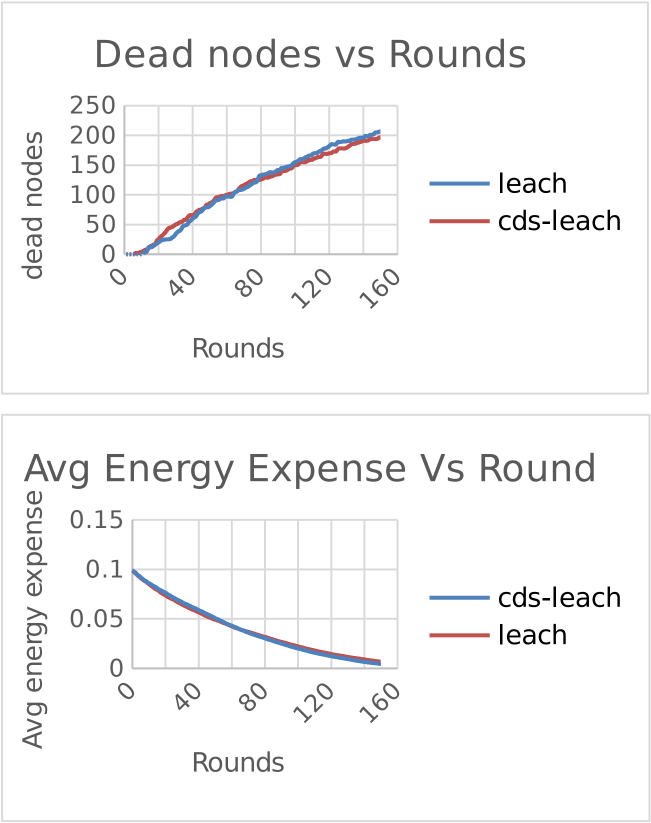
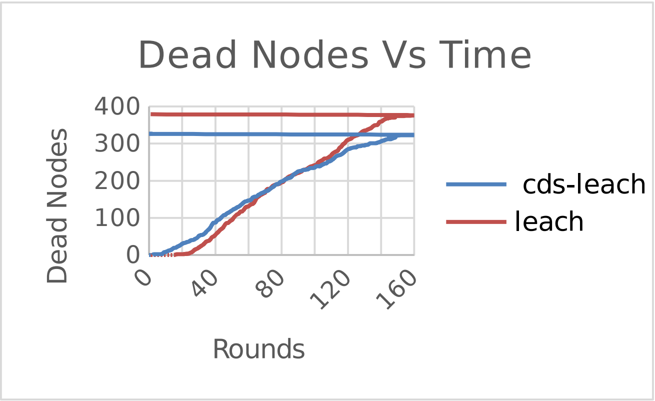


Figure 4: The graph of dead nodes VS rounds and Average energy dissipated VS rounds for 250 node simulation for LEACH and CDS-LEACH

Similarly for 400 node simulation was carried out and the performance graphs are shown below.



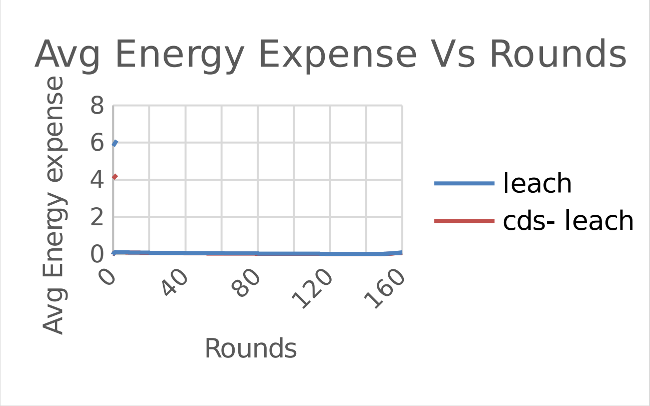


Figure 5: The graph of dead nodes VS rounds and Average energy dissipated VS rounds for 400 node simulation for LEACH and CDS-LEACH

From Figure 4 and 5 it can be easily seen that the performance is not that significant in case of 250 nodes but it becomes quite significant in case of 400 nodes structure.

Below is some of the representative statistics of 250/400 node simulation figures.

Table 2: Statistics of important simulation values

S. No.	Parameters	Protocols	250 nodes	400 nodes
1	First dead node round	LEACH	6	7
		CDS-LEACH	12	13
2	Total energy expended by CHs	LEACH	5.978611	8.113001
		CDS-LEACH	5.924069	6.270837
3	Data Transferred to CHs	LEACH	19007	26902
		CDS-LEACH	19276	27800

The above table depicts the comparison of LEACH and CDS- LEACH parameters. Hence it can be implied that the CDS- LEACH is more energy efficient than that of LEACH.

VI. Conclusions and Future Work

It can be easily seen that merely having the conditions of higher energy in selecting clusters is not energy efficient but having added criteria such as connect dominating set helps in proper dissemination of the data within the cluster .Moreover the energy savings for 400 nodes may be seeming less but this figure may find its significance when the number of nodes cross 1000.

In future work, the intension is to extend this concept of dominating sets in LEACH like protocols TEEN, APTEEN, and HEED etc.

References Références Referencias

1. M. Rai, Sh. Verma, and Sh. Tapaswi, "A Power Aware Minimum Connected Dominating Set for Wireless Sensor Networks," Journal of networks, Vol. 4, no. 6, August 2009.
2. Z. Liu, B. Wang, and Q. Tang, "Approximation Two Independent Sets Based Connected Dominating Set Construction Algorithm for Wireless Sensor Networks," Inform. Technol. J., Vol. 9, Issue 5, pp. 864-876, 2010.
3. D. Estrin, R. Govindan, J.S. Heidemann and S. Kumar, Next century challenges: scalable coordination in sensor networks "Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking", (1999) August 15-20, Seattle, USA.
4. I. Akyidiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, Wireless sensor networks: a survey "Computer Networks", vol. 38, no. 4,(2002).
5. S. Lindsey and C. Raghavendra, Data gathering algorithms in sensor networks using energy metrics "IEEE Transactions on Parallel and Distributed Systems", vol. 13, no. 9 (2002).
6. A. Thakkar and K. Kotecha, "WALEACH: Weight based energy efficient Advanced LEACH algorithm," Computer Science & Information Technology (CS & IT), vol. 2, no. 4, 2012.
7. M. A. Razzaque and S. Dobson, "Energy-efficient sensing in wireless sensor networks using compressed sensing," Sensors, vol. 14, no. 2, pp. 2822–2859, 2014.
8. P. Kumarawadu, D. J. Dechene, M. Luccini, A. Sauer. Algorithms for Node Clustering in Wireless Sensor Networks: A Survey. Proceedings of IEEE 2008.
9. Alan D. Amis, Ravi Prakash, Thai H.P., Vuong Dung, T. Huynh. Max- Min D-Cluster Formation in Wireless AdHoc Networks. Proceedings of IEEE conference INFOCOM 2000.
10. Maniak chatterjee, Sajal. K.das, DamlaTurgut. WCA: A Weighted Clustering Algorithm for wireless adhoc networks. Journal of cluster computing (Special issue on Mobile AdHoc Networks) 2002.
11. Liyang Yu, Neng Wang, Wei Zhang, Chunlei Zheng. GROUP: a Grid- clustering Routing Protocol for.
12. Wireless Sensor Networks. Proceedings of IEEE conference on Wireless communications, Networking and Mobile Computing (WiCOM), 2006
13. Wendi Rabiner, Heinzelman, Anantha Chandrakasan, HariBalakrishnan. Energy- Efficient Communication Protocol for Wireless Microsensor Networks. Proceedings of IEEE 2000.
14. V. Loscrì, G. Morabito, S. Marano.: A Two-Levels Hierarchy for Low- Energy Adaptive Clustering Hierarchy (TL-LEACH). Proceedings of IEEE 2005, 0-7803-9152-7/05.

15. Ossama Younis and Sonia Fahmy. HEED: A Hybrid, Energy-Efficient, Distributed Clustering Approach for Ad-hoc Sensor Networks. IEEE transactions on Mobile computing, Vol 3, No 4, Oct-Dec 2004.
16. P. Kumarawadu, D. J. Dechene, M. Luccini, A. Sauer. Algorithms for Node Clustering in Wireless Sensor Networks: A Survey. Proceedings of IEEE 2008.
17. Benjie Chen, Kyle Jamieson, Hari Balakrishnan, Robert Morris. Span: An Energy Efficient Coordination Algorithm for Topology Maintenance in Ad Hoc Wireless Networks. Wireless Networks 8, 481–494, 2002, Kluwer Academic Publisher.
18. Haowen Chan, Adrian Perrig. ACE: An Emergent Algorithm for Highly Uniform Cluster Formation. Proceedings of the First European Workshop on Sensor Networks (EWSN), Vol. 2920 Springer (2004), p.154-171.
19. Heinzelman, W. Application-specific protocol architectures for wireless networks. Massachusetts Institute of Technology; Cambridge, MA, USA: 2000 (Doctoral dissertation, PhD Thesis).

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 20 Issue 1 Version 1.0 Year 2020
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 2249-4596 & Print ISSN: 0975-5861

Security Investigation on Remote Access Methods of Virtual Private Network

By Peter S. Nyakomitta & Dr. Silvance O. Abeka
Jaramogi Oginga Odinga University

Abstract- Remote access is one of the prevalent business trends in today's computing pervasive business environments. The ease of access to internal private networks over the internet by telecommuter devices has given birth too many security threats to the endpoint devices. The application client software and data at rest on the endpoint of remote access methods such as: Tunneling, Portal, Desktop Applications and Direct Access do not offer protection for the communication between the VPN gateway and internal resources. This paper, therefore investigate the security pitfalls of remote access for establishing virtual private network methods. To address these challenges, a remote access method to secure endpoint communication is proposed. The study adopted investigative research design by use of empirical review on the security aspect of the current state VPN Remote Access methods. This necessitates the review of the research article on the current state and related works which leads to critiques and offer proposed solution to remote access endpoint VPN. The scope of this study is limited to secure virtual private network endpoint data communication. In this paper, an investigation of these access technologies given.

Keywords: remote access, tunneling, portal, desktop application, direct application, gateway.

GJCST-E Classification: C.2.m

SECURITYINVESTIGATIONONREMOTEACCESSMETHODSOFVIRTUALPRIVATENETWORK

Strictly as per the compliance and regulations of:

Security Investigation on Remote Access Methods of Virtual Private Network

Peter S. Nyakomitta [α] & Dr. Silvance O. Abeka [σ]

Abstract- Remote access is one of the prevalent business trends in today's computing pervasive business environments. The ease of access to internal private networks over the internet by telecommuter devices has given birth too many security threats to the endpoint devices. The application client software and data at rest on the endpoint of remote access methods such as: Tunneling, Portal, Desktop Applications and Direct Access do not offer protection for the communication between the VPN gateway and internal resources. This paper, therefore investigate the security pitfalls of remote access for establishing virtual private network methods. To address these challenges, a remote access method to secure endpoint communication is proposed. The study adopted investigative research design by use of empirical review on the security aspect of the current state VPN Remote Access methods. This necessitates the review of the research article on the current state and related works which leads to critiques and offer proposed solution to remote access endpoint VPN. The scope of this study is limited to secure virtual private network endpoint data communication. In this paper, an investigation of these access technologies given.

Keywords: remote access, tunneling, portal, desktop application, direct application, gateway.

Abbreviations: Virtual Private Network (VPN), Layer 2 Forward (L2F), Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), Internet Protocol Security (IPsec).

I. Introduction

An enterprise network normally consists of many remotely connected sites located far away from each other. Traditionally, leased lines connections utilizing frame Relay and Asynchronous Transfer Mode (ATM) were used to provide connectivity among these customer sites. The growth of this network made it become a costly solution and a challenge for network scalability. Virtual Private Network (VPN) came as an alternative which provide flexible solutions, such as securing communication between remote telecommuters and organization's servers, regardless of where telecommuters are located. Sandeep et al, (2016), in their article describe a Virtual Private Network (VPN) as the traditional approach for an end-to-to end secure connection between two endpoints through use of public or shared telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. The VPN establishes tunnels between servers in a site-to-site VPN, clients and servers in a client-to-site VPN (Avani and Ankita, 2017). The approach opted to investigate the security in remote access methods since most large corporations, educational institutions, and government agencies uses VPN technology to enable telecommuter to securely connect to a private network.

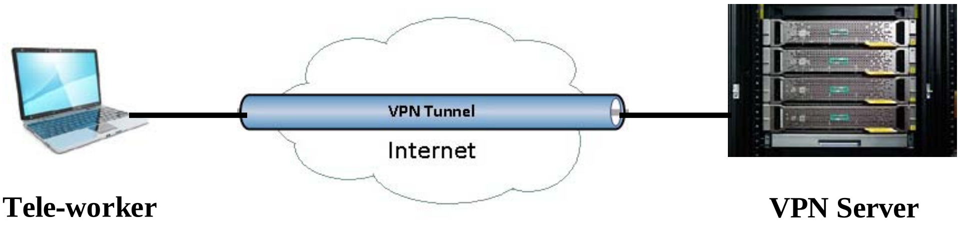


Figure 1: Remote Access VPN Architecture

It can be conceptualized as creating a tunnel from one network to another, with encrypted data travelling through the tunnel before being deciphered at its destination. Telecommuters can connect to their corporate LAN or any other LAN regardless of where the telecommuters are located (Rashikala, 2013). They can access resources such as email and documents as if they were connected to the LAN as normal.

All teleworkers authenticate themselves with the VPN server, which is protected by a firewall. Once a user is connected to the network, an internal firewall guarantees that access is available only to the required resources (Butts and Shenoi, 2011). When a data packet is transmitted from a teleworker, it sends it through a VPN gateway, which adds an Authentication Header for routing and authentication. The data is then encrypted and, finally, enclosed with an Encapsulating Security Payload which contains the decryption and handling instructions.

Author α σ: Department of School of Informatics and Innovative Systems, Jaramogi Oginga Odinga University of Science & Technology, Bondo, Kenya. e-mail: pnyakomitta@yahoo.com

The receiving VPN server strips the header information, decrypts the data, and routes it to its intended destination. A VPN allows the provisioning of a virtual "tunnel" connecting the two endpoints. The traffic within the VPN tunnel is encrypted so that other users of the public internet cannot eavesdrop by intercepting communications (Tarek and Yasser, 2011). By implementing a VPN, a company can provide access to the internal private network to clients around the world at any location with access to the public internet.

Remote access VPN is one of the prevalent business trends in today's ubiquitous computing era which deploy use of secure remote access to corporate resources by establishing an encrypted tunnel across the network. It is a user-to-LAN connection used by a company that has employees who need to connect to the private network from various remote locations. Remote-access VPNs permit secure, encrypted connections between a company's private network and remote users through a third-party service provider.

According to Rajamohan, (2014), they allow secure access to corporate resources by establishing an encrypted tunnel across the Internet. While a firewall protects the systems and data on a LAN from unauthorized access, it does nothing to protect the confidentiality and integrity of traffic traversing the Internet on its way to and from the LAN. That's the role of a virtual private network, or VPN. VPN technology provides encryption and tunneling functions for networked traffic across the Internet. Data is encapsulated in an IP "wrapper" that travels over the Internet. When data is sent, it must be wrapped and encrypted by a gateway using an encryption algorithm. At the other end of the communication link, the destination gateway must "unwrap" the data, decrypt it, and route it to its destination.

II. Remote Access vpn Methods

This section presents the state-of-the-art Remote Access VPN Methods for establishing virtual private network. The remote access methods are most commonly used for teleworkers. This section describe four categories based on their high-level architectures and the security implications. The categories include: tunneling, portals, remote desktop access, and direct application access. The sub-section below gives an investigation of mote access in VPN, as follows.

a) Tunneling

Many remote access methods offer a secure communications tunnel through which information can be transmitted between networks, including public networks such as the Internet. According to Murugiah and Karen, (2016), tunneling involves establishing a secure communications tunnel between a telework client device and a remote access server, often a virtual private network (VPN) gateway buy use of cryptography to protect the confidentiality and integrity of the transmitted information between the client device and the VPN gateway. The VPN gateway can take care of user authentication, access control and other security functions for teleworkers. The tunnel uses cryptographic protocols like IPsec, SSL and SSH tunnels to protect the confidentiality and integrity of the communications. The figure 2.shows the tunneling architecture used to set tunneling remote access.

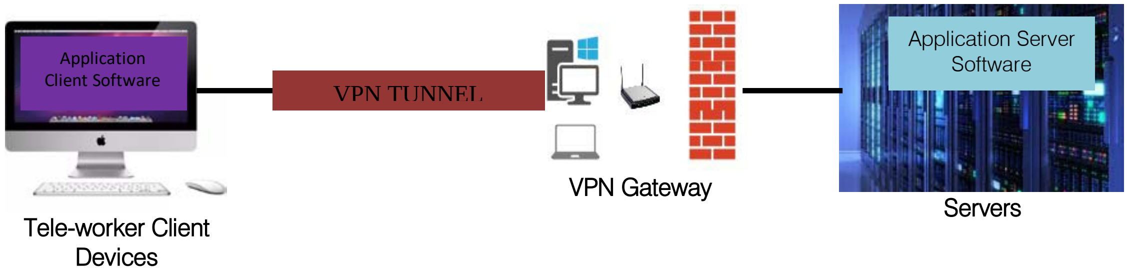

Application Client Software
VPN TUNNEL
Application Server Software
Tele-worker Client Devices
VPN Gateway
Servers

Figure 2: Tunneling Architecture

Once a VPN tunnel has been established between a teleworker's client device and the organization's VPN gateway, the teleworker can access many of the organization's computing resources through the tunnel. To use this application of VPN, users must either have the appropriate VPN software on their client devices or be on a network that has a VPN gateway system on it. The VPN gateway can control access to the parts of the network and the types of access that the teleworker gets after authentication. For example, a VPN might allow a user to only have access to one subnet, or to only run particular applications on certain servers on the protected network. In this way, even though the cryptographic tunnel ends at the VPN gateway, the gateway can add additional routing to the teleworker's traffic to only allow access to some parts of the internal network.

b) Portals Applications

A portal is a server that offers access to one or more applications through a single centralized interface (Murugiah and Karen, 2016). A teleworker uses a portal client on a telework client device to access the portal. The application client software is installed on the portal server, and it communicates with application server software on servers within the organization. The Figure 3 shows the basic portal solution architecture. The portal protects communications between the client devices and the portal, and portals can also authenticate users and restrict access to the organization's internal resources.

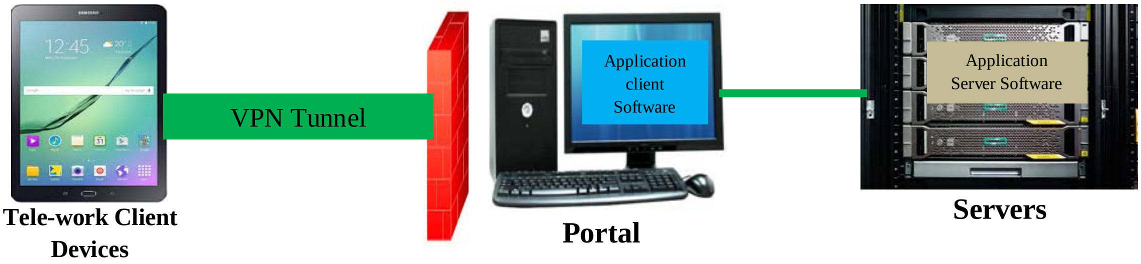


Figure 3: Portal Architecture

In terms of security, portals have most of the same characteristics as tunnels: portals protect information between client devices and the portal, and they can provide authentication and access control. The application client software and data at rest resides on the portal server which then get transferred to the client devices which are then typically stored on the client devices much more temporarily than data for a tunneled solution is. Having the application client software centralized gives an organization more control over how the software and data is secured as opposed to more distributed remote access solutions. Portals limit the access a teleworker has to particular application clients running on the portal solutions.

c) Desktop Application Access

A remote desktop access solution gives a teleworker the ability to remotely control a particular desktop computer at the organization, most often the user's own computer at the organization's office, from a telework client device. The solution allows the user to access all of the applications, data, and other resources that are normally available from their PC in the office. Figure 4, shows the basic remote desktop access architecture.

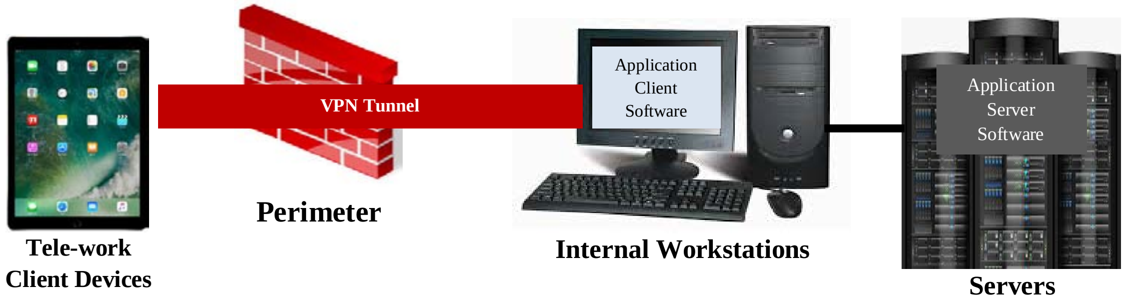


Figure 4: Remote Desktop Access Architecture

Remote desktop access uses a proprietary protocol, Remote Desktop Protocol (RDP) to enables users to interfaces with another computer through a graphical interface. It allows users to gain access to the desktop of another computer. According to (Karen, Paul and Murugiah, 2009), the remote desktop access software protects the confidentiality and integrity of the remote access communications and also authenticates the user to ensure that no one else connects to the internal workstation. However, because this involves end-to-end encryption of the communications across the organization's perimeter, the contents of the communication are hidden from the network security controls at the perimeter, such as firewalls and intrusion detection systems. A remote desktop access client program is installed on each telework client device, and it connects directly with the teleworker's corresponding internal workstation on the organization's internal network.

d) Direct Application Access

With direct application access, remote access can be accomplished without using remote access software. A teleworker can access an individual application directly, with the application providing its own security like communications encryption, user authentication. According to Murugiah and Karen (2016), one of the most common examples of direct application access is Web-based access to email, also known as Webmail. The teleworker runs a Web browser and connects to a Web server that provides email access. The Web server runs HTTP over SSL (HTTPS) to protect the communications and the Webmail application on the server authenticates the teleworker before granting access to the teleworkers email. The Figure 5, shows the high-level architecture for direct application access.

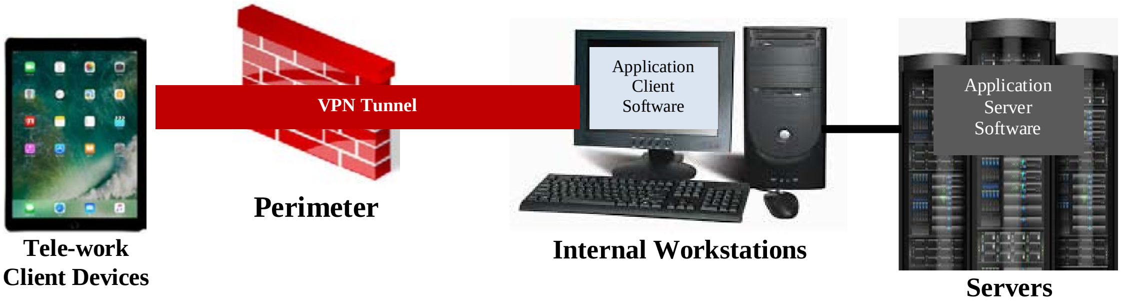


Figure 5: Direct Application Access Architecture

The application client software installed on the telework client device initiates a connection with a server, which is typically located at the organization's perimeter. The direct application access architecture is generally only acceptable if the servers being accessed by the teleworkers are located on the organization's network perimeter or in a public-facing cloud, and not internal networks. Servers that are directly accessible from the Internet should already be well-secured to reduce the likelihood of compromise. Many organizations choose to provide direct application access to only a few lower-risk applications that are widely used, such as email, and use tunnel or portal methods to provide access to other applications, particularly those that would be at too much risk if they were directly accessible from the Internet.

III. Related Work

In (Ernest et al, (2015) proposed advanced technologies to provide tremendous support for network administrators by implementing a secure remote system administration app that runs on android smartphones to aid them administer their servers remotely when they (network administrators) are out stationed using their smartphones. The android app developed in eclipse establishes a secure connection with a remote server running a PHP application. The app was developed based on the Remote Frame Buffer (RFB) protocol. The RFB protocol, a display protocol has some security lapses including being vulnerable to Man-In-The-Middle (MITM) attack using a few tools and techniques (Masthan, Kumar and Prasad, 2013). This paper therefore incorporated a self-signed Secure Socket Layer (SSL) certificate in the android app to enable secure encrypted connections to be established between the android app and the remote server to ensure end-to-end security against attacks such as Man-In-The-Middle (MITM). The secure RFB protocol proposed and implemented in the android app was compared with other existing software for remote system administration such as Remote Desktop (RDP), and RFB protocols using ICMP ping command. The results show that the average response time of the RDP protocol was 436ms, that of the RFB protocol was 496ms and that of the android app which is based on a proposed secure RFB protocol was 474ms. The proposed android app which will act as an interface to the network server will connect to the server using Virtual Private Network (VPN) technology.

With this system, a system administrator can create a user remotely, create, view and modify text files remotely, check network status, shutdown a server and set user privileges. The system was developed based on a proposed secure RFB protocol with self-signed Secure Socket Layer (SSL) certificate incorporated into this RFB protocol to ensure end to- end encrypted connections between the smart device (client) and server. Mobile Devices Management (MDM) applications are developed to address some of the challenges associated with mobile devices (such as policy management, software distribution, and inventory management) that are not related to BYOD security. MDM functionality is similar to that of PC configuration life-cycle management (PCCLM) tools; however, mobile-platform specific requirements are often also included in MDM suites (Gartner, 2014).

On their paper, (Kumari and Khan, 2014) proposed a symmetric key and smart card-based remote user password authentication scheme that was intended to provide anonymity while resisting all known attacks. On their part, (Shehzad et al, 2015). An enhanced privacy preserving remote user authentication scheme with provable security. Security Comm. Networks. 8:3782–3795 proposed a supplemented scheme to overcome security weaknesses of the scheme proposed in (Kumari and Khan, 2014). The authors claim to have analyzed the security of the proposed scheme in random oracle model which confirmed the robustness of the scheme against all known attacks.

A study by (Madhusudhan and Hegde, 2017), pointed out that two robust remote user authentication schemes using smart cards that were claimed to defend against ID-theft attacks, reply attacks, undetectable on-line password guessing attacks, off-line password guessing attacks, user impersonation attack, server counterfeit attack and man-in-the-middle attack. In (Gartner, 2014), the authors discuss that a smart-card based remote user authentication scheme consisting of four phases, which include initialization, registration, login, and authentication has been proposed.

A wireless body area network (WBAN) is a system that provides automatic health monitoring and sends crucial health-related data remotely to the doctors with the help of body sensors. The protection of these health records is therefore very critical to prevent malicious and fraudsters accessing these data and impersonating the patients. These networks have an authentication system as their backbone because a lapse in such technologies could lead to the death of a patient. In (Salama, Taha, and Elmahdy, (2015), a scheme known as PMAS is proposed for mutual authentication between the sink (patients' personal cellular phone) and sensor nodes focused on the advanced idea behind the Diffie-Hellman key exchange scheme. Here, a trusted third party (TTP) distributes keys (public and private) to the medical sensor node and sink (mobile / cellular phone).

Recently, elliptic curve cryptography (ECC) has been implemented widely in multi-factor authentication. It is basically a public key encryption technique based on elliptic curve theory that can be used to create smaller keys, which yields faster and more efficient algorithms as a result (Chande, et al, 2016). It was developed to reduce computational costs while providing the same level of security as other similar operations such as modular exponentiation and it finds applications in authentication protocols involving smart cards, RFIDs, wireless networks, digital signatures and other authentication techniques.

IV. Critique of the Current Remote Access Technologies

The four remote access methods discussed above were noted to have a number of security setbacks that render them ineffective in VPN deployments. To start with, Tunneled IP traffic may not receive the intended level of inspection or policy application by network-based security devices unless such devices are specifically tunnel aware. This reduces defense in depth and may cause security gaps. This security weakness applies to all network-located devices and to any end-host-based firewalls whose existing hooking mechanisms would not show them the IP packet stream after the tunnel client does decapsulation or before it does encapsulation. In addition, IP addresses inside tunnels are not subject to ingress and egress filtering in the network they tunnel over, and hence may allow malicious content into internal networks. Moreover, if the encapsulated IP packet specifies source routing beyond the recipient tunnel client, the host may forward the IP packet to the specified next hop. This may be unexpected and contrary to administrator wishes and may have bypassed network-based source routing controls.

On the part of portals applications, Tomas (2014) point out that they are faced with challenges regarding authentication including user identification, authorization, auditing or logging and session management. Desktop application access face screen sharing security setback that allow an attacker to penetrate an enterprise's defenses. In addition, many enterprises permit or fail to regulate the use of third-party file storage services to facilitate remote access to data, and when files end up in cloud-based repositories, enterprises lose control. On its part, direct application access requires the use of IPv6 exclusively to distribute addressing to connecting endpoints. This presents a larger management problem when it comes to client addressing and identification.

Due to the setbacks noted in the four access methods discussed above, a number of protocols have been developed to address some of these challenges. Unfortunately, these protocols also introduce vulnerabilities that render them insecure. For instance, the RFB protocol, a display protocol has some security lapses including being vulnerable to Man-In-The-Middle (MITM) attack using a few tools and techniques (Ernest et al, 2015). Despite the fact that RFB protocol uses encrypted passwords and network, any communication over the network is vulnerable and can be attacked by a Man-In-The-Middle (MITM) by using a few tools and techniques. In addition, the applications of VNC which are developed based on RFB protocol are generally slower, offer fewer features and security options than Remote Desktop (RD) which is based on the RDP protocol (Masthan, Kumar and Prasad, 2013). Though the data sent between the server and client is encrypted, the RDP protocol may be prone to Man-In-The-Middle attack because there is no verification of the identity of the server when setting up the encryption keys for a session.

Although businesses are mainly concerned with maintaining security, employees are worried about preserving the convenience they need to work from their mobile devices, as well as the privacy they expect regarding the personal information on the device (Morufu et al, 2015). One of the biggest challenges for organizations is that corporate data are being delivered to devices that are not managed by the IT department. This has security implications for data leakage, data theft, and regulatory compliance. Thielens, (2013), noted that the real BYOD challenge is security and that the real security challenge is not actually about the devices, it is about controlling access from the devices to the corporate data. Moreover, Vignesh and asha, (2015), points out that sensitive data on organization and personal data are present in these devices and such any attack on these devices can expose these data.

Many enterprises view most of the MDM applications as a solution to the security challenges of BYOD. However, MDM does not completely address the security challenges of BYOD. MDM does not prevent a hacker from attacking an employee's device or a thief from stealing it and accessing sensitive data. Data leakage, distributed denial of service (DDoS), and malware are the most challenging security threats to BYOD (Gartner, 2014). Further, Manmeet, Chen and Zakiah, (2017), explain that security threat in the paradigm of BYOD creates a great opportunity for hackers or attackers to find new attacks or vulnerabilities that could possibly exploit the students' mobile devices and gains valuable data from them.

Gokulakrishnan, Jayanthi, and Thulasi, (2014) point out that VPN does not provide strong user authentication by default. This means that users can enter a simple username and password to gain access to an internal private network from home or via other insecure networks. On its part, the Point-to-Point Tunneling Protocol (PPTP) which is the most widely supported VPN protocol among Windows users establishes the tunnel, but does not provide encryption (Alshalan et al 2016). In their paper, Muhammad et al, (2016) discuss that a number of users employ mobile VPN clients to either circumvent censorship or to access geo-blocked content, and more generally for privacy and security purposes. Their experiments reveal that several instances of VPN applications that expose users to serious privacy and security vulnerabilities, such as use of insecure VPN tunneling protocols, as well as IPv6 and DNS traffic leakage. In addition, a number of mobile VPN applications actively perform TLS interception while other applications inject JavaScript programs for tracking, advertising, and for redirecting e-commerce traffic to external partners.

Another study by Varmarken et al, (2015), pointed out that some VPN applications implement tunneling protocols without encryption despite promising online anonymity and security to their users. In addition, it was noted that other VPN applications do not tunnel IPv6 and DNS traffic through the tunnel interface respectively due to lack of IPv6 support, mis-configurations or developer-induced errors. Both the lack of strong encryption and traffic leakages can ease online tracking activities performed by in-path middle-boxes such as commercial WiFi APs harvesting user's data and by surveillance agencies.

As Shehzad et al, (2015) points out, a symmetric key and smart card-based remote user password authentication scheme that was intended to provide anonymity while resisting all known attacks is still vulnerable to anonymity violation attack as well as smart card stolen attack. Chin-Ling et al, 2018) demonstrated that schemes that the two robust remote user authentication schemes using smart cards are still vulnerable to ID-theft attack, off-line password guessing attacks, undetectable on-line password guessing attacks and user impersonation. This is particularly true in situations where the user lost a smart card or the malicious legal user. In addition, the smart-card based remote user authentication scheme consisting of four phases has been shown by Gartner, (2014) to be vulnerable to offline password guessing attack under their non-tamper resistance assumption of the smart cards; and it fails to provide forward secrecy.

The challenge of the WBAN authentication is that TTP distributes all the credentials without applying any cryptographic functions or any mathematical computations. It dictates that the insider person can identify different keys of various users easily. Once important credentials are available with any malicious internal person, then he/she can distribute confidential data to others illegally.

Swapnoneel and Chanchal, (2017) point out that mutual authentication has been introduced in remote user verification and access control. However, a password can be compromised during transmission if an efficient scheme is not followed. To address this problem, elliptic curve cryptography (ECC) has been implemented widely in multi-factor authentication. However, the computational cost of one bilinear pairing (an important operation of ECC) is about twice as high as that of one modular exponentiation operation at the same security level. Therefore, the computationally-intensive nature of ECC leaves a security loophole in the protocols that use it. An attacker can force the server or client to repeatedly perform ECC operations in order to clog them, resulting in one or all of them wasting resources by performing unnecessary computations.

V. Proposed Solution

In recent years, mobile devices have replaced desktop personal computers as the primary computing platform for many users. This trend brings to the workplace where nowadays the employees use their personal owned mobile devices to access company's data. BYOD causes a lot of cyber-attacks towards the users and the organization. The proposed solution for BYOD addresses the shortcomings noted in some of the remote access technologies such as platform integrity that lacks in tunneling, authentication such as user identification, authorization, auditing or logging and session management that lacks in portals applications, regulation of file storage services to facilitate remote access to data, a feature that is missing in desktop application access, client addressing and identification that is lacking in direct application access as shown in Figure 6 below.

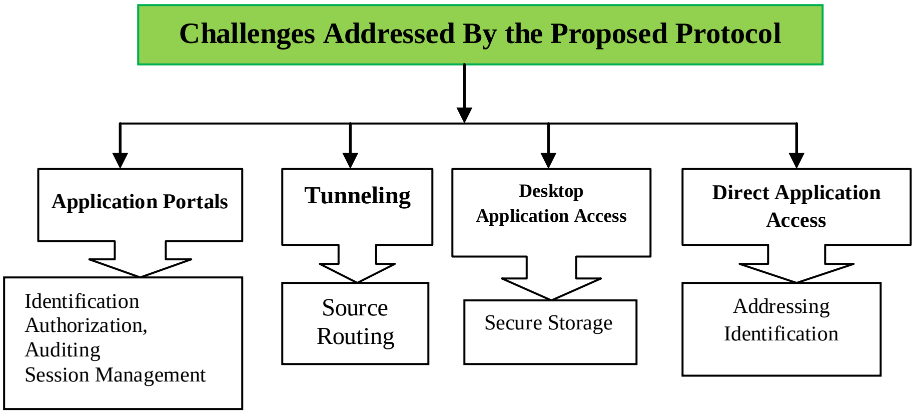


Figure 6: Problems Addressed By the Proposed Protocol

a) Architecture of the Proposed Protocol

The conventional remote access technologies have been noted to have a number of setbacks related to identification, authorization, auditing, session management, source routing, secure storage and addressing. Figure 7 shows the architectural design of the proposed protocol. As this figure shows, the proposed protocol will comprise of six attack prevention mechanisms namely IP scanning, hashing, MAC and IP based identification and addressing, digital certificates, one time passwords (OTP) and logging capability. IP scanning will be effective against source routing attacks where attackers make use of intranet IP addresses so as to fool the firewall against inspecting the traffic utilizing these internal IP addresses.

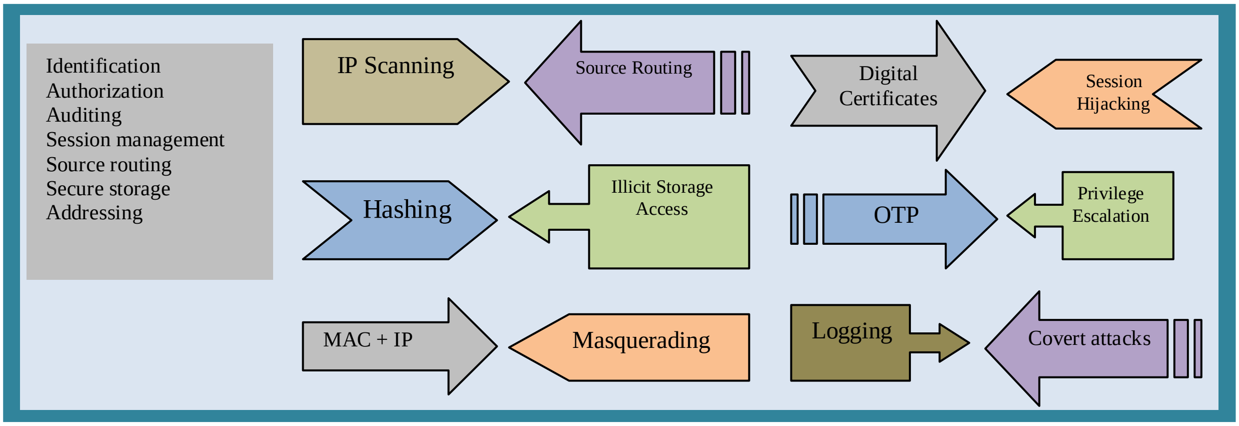


Figure 7: Proposed Protocol Architecture

The other salient feature of the proposed protocol is its hashing activity for any requested storage access to ensure secure storage of this vital organizational resource. To prevent masquerading attacks using false identification and addressing, the proposed protocol will utilize a combination of media access control (MAC) and IP address of the client and server machines for identification and addressing. Session management will be secured using digital certificates that will serve to protect the VPN communication against session hijacking attacks. On the other hand, one time passwords (OTP) will be instrumental in curtailing privilege escalation for authorized users such that once they accomplish any authorized activity, they require another set of authorization for the next activity. Covert attacks will be prevented by the proposed protocol's logging feature that will facilitate auditing during forensic analysis.

b) Secure Remote Access Method (SRAM)

Table 3.2 confirms that to secure VPN connections, a layered protection approach is necessary. The proposed VPN protection protocol will be implemented in all the four layers of the TCP/IP stack. Figure 3.2 shows the implementation design of the proposed protocol

Table 3.2: Layered Attacks and their likely target

TCP Layer	Attacks to be Prevented
Application Layer	Fingerprinting, Reconnaissance
Transport Layer	Modifications, replay
Network Layer	Source routing, packet redirection
Physical Layer	Masquerading attacks

As this figure illustrates, the proposed Secure Remote Access Method (SRAM) will be implemented in the region between the VPN end devices and the firewall. This is because the packets moving in the regions between the two firewalls are protected by SSL and TLS via the VPN tunnel.

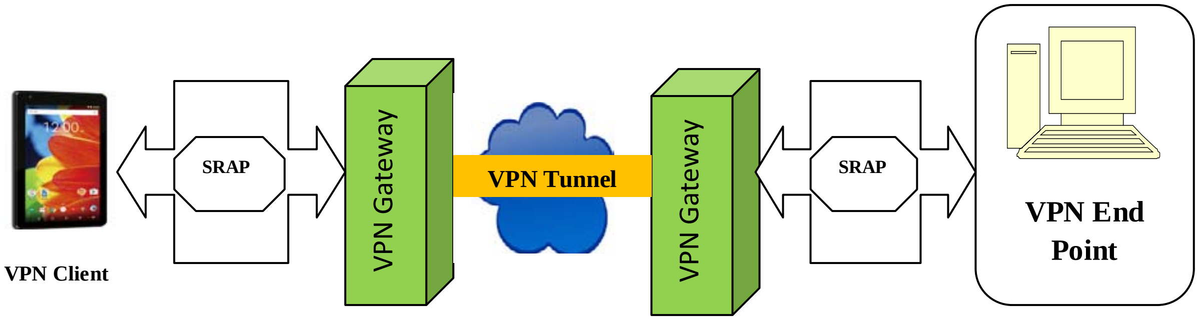


Figure 8: Proposed Secure VPN Access Method

As such, most attacks are only possible immediately these packets exit the tunnel and are passed through firewalls. All the layered protection discussed above will therefore implemented in the regions between firewalls and VPN endpoints (VPN client and VPN server).

VI. Conclusion and Recommendation

In this study, an investigation of remote access methods for establishing virtual private network a has been carried out. From this examination, it has been noted that all of them fall short of endpoint security, making it possible for attackers to carry out unauthorized data transfers from their victim machines due to lack of cryptographic protocols for securing the data that reside at the client device.

Towards the end of this paper, a protocol that could potentially address the security gap endpoint remote access client devices has been provided. One of the pillars of this protocol is encryption that would help enciphered the content of the data at the endpoint device and secondly component of this protocol is the dual-factor authentication that will requires the presence of two or more factors to prove the authenticity of the account holder. Owing to its security entropy, this protocol is therefore recommended for implementation in remote access methods for establishing virtual private network.

References Références Referencias

1. P. Sandeep et al, (2016). "A Survey of Mobile VPN Technologies." IEEE Communications Surveys & Tutorials 18.2 (2016): 1177-1196.
2. P. Avani and G. Ankita (2017), A Survey of VPN Performance Evaluation. International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169, Volume: 5 Issue: 5, pp 409 – 413
3. W. Rashikala, (2013). An Empirical Test-bed Analysis of a Virtual Private Network Protocol. UNITEC Institute of Technology, New Zealand.
4. J. Butts and S. Shenoi (2011): Critical Infrastructure Protection V, IFIP AICT 367, pp. 185–199,
5. S. Tarek and A. Yasser, (2011). Effective and Extensive Virtual Private Network. Journal of Information Security, 2011, 2, 39-49.
6. P. Rajamohan (2014).An Overview of Remote Access Vpns: Architecture and Efficient Installation. Ipasj International Journal of Information Technology (Iijit).
7. S. Murugiah and S. Karen (2016), Guide to Enterprise Telework, Remote Access, and Bring Your Own.S. Karen, H. Paul and S. Murugiah (2009). Guide to Enterprise Telework and Remote Access Security. National Institute of Standards and technology.
8. S. Murugiah and S. Karen, (2016).Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. NIST Special Publication 800-46 Revision 2.
9. Device (BYOD) Security. NIST Special Publication (SP) 800-46 Rev. 2.
10. D. Ernest et al, (2015).A Comparative Study Of Remote Access Technologies and Implementation of a Smartphone App for Remote System Administration Based on a Proposed Secure RFB Protocol. International Journal of Science and Engineering Applications. Volume 4 Issue 4, pp. 163-168.
11. K. Masthan, S. Kumar and V. Prasad, (2013) Virtual Network Computing of User Appliances. International Journal of Computer Science and Mobile Computing. Volume 2, Issue 8. pp. 132.
12. Gartner. (2014). Gartner says less than 0.01 percent of consumer mobile apps will be considered a financial success by their developers through 2018. Gartner Newsroom.
13. S. Kumari and MK. Khan, (2014). More secure smart card-based remote user password authentication scheme with user anonymity. Security and Communication Networks 2014; 7(11): 2039–2053.

14. A. Shehzad et al, (2015). An enhanced privacy preserving remote user authentication scheme with provable security. Security Comm. Networks. 8:3782–3795.
15. R. Madhusudhan and M. Hegde, (2017). Security bound enhancement of remote user authentication using smart card. J. Inf. Secur. Appl. 2017, 36, 59–68.
16. H. Salama, S. Taha, and H. Elmahdy, (2015). PMAS: A proposed mutual authentication scheme for wireless body area networks. In Information and Communication Technology Convergence (ICTC), 2015 International Conference on (pp.636-641). IEEE.
17. Chande, et al, (2016). A CAE Scheme Using ECC Based Self Certified PKC. J. Comput. Sci. Vol. 12, pp. 527–533.
18. O. Morufu et al, (2015). A Review of Bring Your Own Device on Security Issues. SAGE Open. Pp. 1-11.
19. J. Thielens, J. (2013). Why API are central to a BYOD security strategy. Network Security, 2013, 5-6. doi:10.1016/S1353- 4858(13)70091-6.
20. U. Vignesh and S. Asha, (2015). Modifying security policies towards BYOD. 2nd International Symposium on Big Data and Cloud Computing. Vol.50, pp. 511 – 516.
21. Gartner, (2014). Gartner says less than 0.01 percent of consumer mobile apps will be considered a financial success by their developers through 2018. Gartner Newsroom.
22. M. Manmeet et al, (2017).Security and Privacy Risks Awareness for Bring Your Own Device (BYOD) Paradigm. International Journal of Advanced Computer Science and Applications. Vol. 8, No. 2, pp. 53-62.
23. J. Gokulakrishnan and V. Thulasi, (2014). "A Survey Report On Vpn Security & Its Technologies." Indian Journal of Computer Science and Engineering (IJCSE) 5.4 (2014): 3-5.
24. A. Alshalan, et al, (2016). "A Survey of Mobile VPN Technologies." IEEE Communications Surveys & Tutorials 18.2 (2016): 1177-1196.
25. I. Muhammad et al, (2016). An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps. IMC. Pp.1-16
26. Varmarken et al, (2015). AntMonitor: A System for Monitoring from Mobile Devices. In ACM (C2B(I)D), 2015.
27. A. Shehzad, (2015). An enhanced privacy preserving remote user authentication scheme with provable security. Security Comm. Networks. 8:3782–3795.
28. C. Chin-Ling et al, (2018). An Improvement on Remote User Authentication Schemes Using Smart Cards. MDPI. 7, 9; pp. 1-19.
29. R. Swapnoneel and K. Chanchal, (2017). Cryptanalysis and Improvement of ECC Based Authentication and Key Exchanging Protocols. MDPI. Vol.1, Issue 9, pp. 1-25.

This page is intentionally left blank

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 20 Issue 1 Version 1.0 Year 2020
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 2249-4596 & Print ISSN: 0975-5861

The Media Layers of the OSI (Open Systems Interconnection) Reference Model: A Tutorial

By Koffka Khan
The University of the West Indies

Abstract- The Media Layers of the open systems interconnection (OSI) reference model convert bits to packets. It is a very important aspect of network communication and consists of various networking protocols. At the lowest level the physical layer deals with Media, Signal and Binary Transmission of Bits. Then there is the Data Link layer which deals with media access control (MAC) and logical link control (LLC) Physical Addressing of Frames, for example Ethernet. Finally, there is the Network layer which deals with Path Determination and IP Logical addressing of Packets. This article gives a review of these Media Layers and will contribute to adding knowledge for a networking novice while consolidating concepts for an experienced professional or academic.

Index Terms: *media, layers, OSI, physical, bits, data link, frames, ethernet, network, packets.*

GJCST-E Classification: *C.2.0*

The Media Layers of the OSI (Open Systems Interconnection) Reference Model: A Tutorial

Koffka Khan

Abstract- The Media Layers of the open systems interconnection (OSI) reference model convert bits to packets. It is a very important aspect of network communication and consists of various networking protocols. At the lowest level the physical layer deals with Media, Signal and Binary Transmission of Bits. Then there is the Data Link layer which deals with media access control (MAC) and logical link control (LLC) Physical Addressing of Frames, for example Ethernet. Finally, there is the Network layer which deals with Path Determination and IP Logical addressing of Packets. This article gives a review of these Media Layers and will contribute to adding knowledge for a networking novice while consolidating concepts for an experienced professional or academic.

Index Terms: media, layers, OSI, physical, bits, data link, frames, ethernet, network, packets.

I. Introduction

We first talk about being globally connected, then we're going to take a look at the internet, then we're going to look at the network as a platform and then we're going to look at the changing Network environment. So, what does globally connected mean in today's world? We are being increasingly connected more than any time in human history. The globe is getting smaller (not the actual earth!!!) but we as a people are able now to communicate around the globe in real time, whereas we weren't able to do that a hundred years ago. You know if you go back to about 1900 in the United States it would take you about one week to send a letter across the United States. But in today's world we have communication with cell phone technology, or we have chat technology, or we collaborate on videos or we can chat to with each other with text and there are people from the UK from Canada from United States and from New Zealand and Australia and we all communicate together and collaborate. So, the network really has no boundaries! We live and work in a global community, we communicate together through networks and on a global basis and we work, and we play together.

Let's take a look at what allows us to connect together globally. Networks connect us together. Networks come in many different sizes. We can have a small home office network where you might connect two or three different computers to a printer over a Wi-Fi link [58]. You might also have a file server [34]. However, you might not have a web server [24] on a home office or an office network but on a medium to large networks you are going to have those different devices. You're going to have some type of email service for email, a server for web clients etc. All these devices can be connected using a switch. You may have a router then that sends messages out of the network and again you'd have print sharing and file sharing [45], [66].

In this paper you would learn about clients and servers and what are clients and servers [8]. When you're talking about networks and when we hear the term client and server where the client is not necessarily a PC and a file server which is a very powerful computer. The term client and server typically means when you've got a client requesting information and the server provides that information. This model involves tow computers. Therefore, you in that could have two different computers "talking" to each other. One is requesting information from another (e.g. the file server). Note that in some network environments a computer "acts" as a server because it's serving up a file. It doesn't necessarily have to be a physical large server. Hence, in this case the two communicating machines (M2M or machine to machine communication [4], [13]) can be two different devices requesting information from each other.

When we talk about peer-to-peer networks [62] where you have devices that are connected without some type of server in place each computer can be both client and server. There are advantages and disadvantages to either client-server or peer-to-peer communication architectures. One advantage of peer-to-peer is that it's easy to set up and is low cost. To set up doesn't take a lot of equipment and it doesn't take a lot of knowledge to be able to set up a peer-to-peer network. However, the security is not as good as you are not able to scale to a larger network easily. You're going to have to then go in and put routers in and create different setup connections.

When we're talking about different network components, you're going to hear the term end devices. End devices are those devices that are requesting information. They can be a computer, a mobile device [60], a tablet [57], or a Smart Watch [36]. An intermediary device are those devices that connect endpoints together or connects an endpoint to another network. They connect the individual end devices to the

Author: Department of Computing and Information Technology, The University of the West Indies, Trinidad and Tobago, W. I.
e-mail: koffka.khan@gmail.com

network and they ensure data flows across the network by providing connectivity. Examples of an intermediary device is a switch. Network media allows us to transmit that data we are transmitting ones and zeros. You'll learn about the OSI model [53] but the OSI model and the TCP/IP model [25] illustrates how the data gets broken down into ones and zeros. Once it gets broken down into ones and zeros it is transported across the network via various types of network media. Your media is going to be anything from the wireless or your wired cable that you have. You might have copper (category 5e or cat6 or coax) [10] or fiber optics [55] or wireless [74] or radio (Bluetooth) [9] to transmit over. You should familiarize yourself with the different networking icons and what they look like [20].

The network represented by physical and logical models. A physical model actually shows how devices are connected together while the logical model shows your IP addresses and information needed for computer to communicate. Thus, you have two different type of topology diagrams. The physical diagram shows the devices and then you have logical shows you the communication information that might be your IP address that might be your IPv4 address [42] and your IPv6 address [33]. There are different types of networks. You have Local area networks (LANs) [61]. A LAN usually span across a small geographical area. If you're in a classroom on a college campus or you're at a small cafe shop or you go to someone's house (they have three or four computers set up at their house) or in a small office are all examples of local area networks (LANs). All the computers can see each other, usually the devices are all interconnected together. At a house you can have a router that comes into your ISP provider [56] or cable provider [2] and then it gets sent to different devices. One can be for video gaming which forms its own local area network and then you can have the rest of the house into an another separate local area network so other family members can all “see” each other and can share files between computers or all persons can print to the same device that's usually going to provide some type of high-speed bandwidth to internal devices.

A wide area network (WAN) [16] connects multiple LANs together. You can kind of think of the Internet as a LAN because it's a lot of local area networks that are connected together. You might think of a college campus. Let's say that a college has three or four different locations and with those locations you're going to connect various LANs or different buildings together and then you're going to have a campus area network (CAN) [43]. There are more network types for example a metropolitan area network (MAN) [16] which might be a city that's connected together. The internet can be considered a large wide area network (WAN) but it's a worldwide collection of interconnected networks. The internet isn't one just one big network it's a bunch of networks connected together—a Network of Networks! and it's not owned by any one individual or group or country. It's really all of them connected together example you might have a government LAN that's connected into intermediary devices, you might have a branch LAN for a company, you know somebody at home is getting connected through their ISP (Internet Service Provider), you might have schools and you might have a large corporation maybe International Business Machines Corporation (IBM) is connecting into the internet or their ISP and so forth.

A company’s intranet means that communication is going to be only available internally. If you have your security set up properly no one outside the company is supposed to access company information. Extra nets [78] are not open to the public. They are opened up to the internal business then suppliers, collaborators, customers. You might have to have some type of login if you log into a portal into your college that you're attending.

When we're talking about how we connect to the Internet we have different types of connectivity. I've already mentioned the ISP which is an Internet service provider. That's a company that connects into a faster connection they have usually have some kind of fiber-optic system coming in to their local supply so for example where you live in the town then AT&T maybe your service provider and they have run cable from their main headquarters out to all the different homes and they pretty much can have all monopolies in your area. There is a DSL company but they're not very they can't really compete on speeds and there's a there's another company that offers a broadband wireless that you can put an antenna on your home or Digicel providing broadband cable [7]. Note that high-speed is not necessarily broadband and broadband is not necessarily high speed. Broadband just means that it's not the old plain old telephone the telephone system (POTS). It is usually coax or fiber optic cable. Broadband cable means you have broadband digital subscriber line or DSL [79] using the older copper phone lines. You might have Wireless that's connects to some mobile devices. Business DSL [54] is not much different than digital subscriber or broadband customers. It's usually the same lines but it is sometimes put in a different category. You can do leased lines and that's where you may have a company those might run anywhere from you know anywhere from $250 a month maybe up to $1,000 a month depending on where you are (location you live in) and those give you much faster access to the Internet. You can lease multiple lines so that you can have multiple company and then you also have Metro Ethernet [59]. Some towns local power company does provide some fiber optics to particular areas. However, they may not run it all the way to the city. Google is putting Google Fiber [3], [73] in two different cities if you're lucky enough to be in one of those cities you can get fiber optics from there and then the different types of Internet connections e.g. to a home or small office home office or business.

We use the term network as a platform where we talk about the term converged networks. The term converged means that things are being meshed together in traditional separate networks. Each network had its own rules and regulations. In pervious networks you have a network that only did email, you had a network that only did file service or only did the database and that was it. However, the converging network allows us to connect to devices that they have their own technology, that it's capable of delivering data voice, video over the same network infrastructure. Thus, when you hear the term converging network it means everything's being merged into the same network. It's using the same media so you don't put one line in for just doing an email server and interconnect endpoint devices and you're going to have totally different lines for your phones. We just don't do that anymore!!! Where are the converged network? The converged network may have a cat5e or cat6 cable coming in it, goes out to the desktop and it goes into the phone and then the phone connects over to the desktop and then that they all get the same Internet through a router. So the same cable is used. You have some type of medium that goes out and it's the devices and the messages that get sent on the same medium so that's the converged network.

There's four characteristics of a network architecture. The first one that you need to have is fault tolerance. Fault tolerance just means that it's not going to go down on you or there's backup to it so if you have multiple lines going to a server for example in a fault tolerant server you might have multiple power supplies so if one power supply goes down it runs on the backup or you may have two network cards into a server so you've got one as a backup. Lack of Scalability means that you can't upgrade that network and put more in devices on it without having to upgrade the major infrastructure. Scalability means that you put things in place so let's say that you put a router and you know a 24 port switch in place. You know Jim only have ten devices on it to begin with, well you know that you can scale all the way up to 24 devices on that switch without having to go and purchase a new switch. That's scalability. Quality of service (QoS) [41], [17]means that you're going to get is consistent bandwidth so for example if you know that you're supposed to be pushing 75 megabits of download speed you're going to consistently get 75 megabits of download speed that's an example of quality of service. Security is the last component and is a very important part of the whole overall network structure.

Bringing your own devices to work or to your workplace or to the college has become very popular in recent years. In the past companies didn't like employees bringing their own devices their own cell phones or iPhones. However, companies have realized that bringing your own device is OK and be able to get on the network because it keeps them from having to purchase it and it keeps them from having to support it other than just the connection to the internet or to the to the network yet allows for online collaboration. Online collaboration is growing e.g. Google Hangouts [15] or YouTube streaming. YouTube stream is essentially an online collaboration because in University students can come into that live stream and they can ask questions and the lecturer can answer those questions in live time on 2-way video communications. You've got Skype and Zoom etc. We have cloud computing where you can put your servers in the cloud. We have Amazon services; you've got Google services and Microsoft services. Cloud services [39] means don't have to store them locally. Cloud computing is putting your information up somewhere other than your local machine where others can access it.

Smart homes and the Internet of Things (IoT) [69] are some trends in technology where household devices communicate to each other and the outside world. You can connect on the Internet then you can put in devices on your refrigerators to monitor and buy your food. Power line networking uses the existing electrical wiring to connect devices together. Whether you realize you could do that or not the existing electrical wiring is copper wiring and you can then send your ones and zeros or you can send your network across the same electrical wiring and then we have wireless broadband. Now that's where you have a wireless internet service provider as you might put an antenna on your house that broadcast that across a wireless broadband service using cellular technology. Cellular technology also allows you to connect to the internet. If you don't have Wi-Fi you can turn your Bluetooth on and then broadcast over to your tablet and or even laptop. If you could get internet on your laptop you could use Bluetooth tethering [29] to get internet on your phone.

II. Communication and Network Protocols

We're going to talk about rules of communication, we're going to talk about network protocols and standards and we're going to look at data transfer in the network. Why do we have rules of communication? What do we call rules? What are they? If we're going to communicate between two different languages and I want to speak to someone in English or in French and someone that's French wants to speak to me in English or from French to English. We must establish rules of how we're going to communicate. If I don't speak French and they don't speak English, then we're not going to be able to communicate. We must establish common rules for instance when we speak, we're going to use French or we're going to use

Spanish. Let's say that we both speak Spanish, but the French-speaking person does not speak English and I don't speak French but we both speak Spanish so we're going to establish rules that when we communicate with each other we're going to use Spanish. That's an example of establishing rules in the networking world. We established rules and there's a group of people that get together and they establish rules. For example, let's assume there are two different networks and group says that they we're going to put this network together. They are going to set chosen protocols up, rules that are going to happen (so the rules that we establish in networking is that we identify the sender and receiver so we need to know who the sender is and we need to know who the receiver is), we need to have a common language and grammar, we need to have the speed and timing of the delivery established and we need confirmation or acknowledgement of requirements (if that's required then we look at message encoding: how are we going to encode those messages so that they can be sent through the system).

The process of converting information into another acceptable form is the message encoding. When a message goes from your computer to the wire or to a wireless medium, we need to know how that message is going to be encoded or translated, the message formatting and encapsulation, the message size, the message timing, the message delivery options is it going to be uncast multicast or broadcast.

We've established our rules now we're going to look at protocols and standards. We need to have protocols and standards because we need to let things work together. We're going to have a common 'thread' so devices can communicate with each other. The rules that govern communications are called protocols. Let's say that we're going to have an official meeting between two politicians, and we stablished protocols beforehand. We say when those politicians meet, they're going to shake hands then they're going to take pictures then they're going to talk with each other for 15 minutes and then then they're going to do another photo op. That's protocols we're establishing, what's going to happen. In the world of networking the role of protocols [22] we establish is how the message is formatted and structured, it's the process by which networking devices share information about pathways with other network and it's how and when error system messages are passed between devices. The protocol also does the setup and termination of data transfer sessions. The protocol interaction would be for example between a web server and a client. For example, we establish a protocol and I have a computer and I open up a browser and that browser has certain protocols to say okay I'm going to want a web page pull down to my computer. Well there's certain protocols in place to say I need it in a particular format for instance, I need it in HTML [44] format and so it establishes those protocols to do that. We have a client it goes through the Internet of the cloud and it sends a packet of information and it says I need to get information from this web server, so the protocol stack says we're going to use HTTP (Hypertext Transfer Protocol) [46]. We're going to use Transmission Control Protocol (TCP) [68] and then Internet Protocol (IP) [70] and then we're going to go across the Ethernet so that's our set of protocols or how they are established.

We have protocol Suites and there's been a number of them. The TCP/IP is an open standard [28]. The TCP/IP is the one of the most common that we use today in networking. The TCP/IP models have your application layer, your transport layer, your internet layer and your network access layer. In each layer you have these different protocols that we set up for example you know at the application layer we set up DNS [50]or you set up by FTP [27] or HTTP and then down at the network access layer you set up Ethernet to be able to go across your medium.

Standards organizations like the International Organization for Standardization (ISO) [31] sets up open standards. There are some advantages to open standards are that they can be easily adopted by anybody, they're not controlled by any one person because they're put out on the market. We still have organizations that get together and they regulate open standards. The TCP/IP model benefits by having a reference model (OSI model). The Open Systems Interconnection (OSI) [81] is layered and provides a list of functions. There are seven layers. It describes the interaction between the layers. You do need to memorize the OSI and TCP/IP models if you're going into networking. There are relationships between the two models for example you have the top three (five six and seven) of the OSI model have been collapsed into the application layer on the TCP/IP side and the transport layer is the same, the network layer is called Internet on the TCP/IP and the bottom two (the data link and the physical layers) have been collapsed into the network access layer. Thus, the TCP/IP model is not simpler, it's just collapsed down into four layers instead of seven.

When we transfer data, we have to put it onto the medium and we have to send it along. We can't just send a whole bunch of ones and zeros as the receiving side needs to know when each individual packet is finished. It needs to know what requests came from who or in what order else all those ones and zeros would just get me garbled and the receiver wouldn't be able to make sense of anything. It wouldn't be able to communicate. Thus, based on our protocols we say we're going to have message segmentation (segmentation means that we're going to break that communication into pieces) so we're going to take those ones and zeros and we're going to segment them out into little blocks. Multiplexing [1] is another term (also called interleaving) the pieces which means that they can arrive at different times and then be put back.

Multiplexing is a method by which multiple analog or digital signals are combined into one signal over a shared medium. A protocol data unit (PDU) is a single unit of information transmitted among peer entities of a computer network. A PDU is composed of protocol specific control information and user data. Encapsulation is a method of designing modular communication protocols in which logically separate functions in the network are abstracted from their underlying structures by inclusion or information hiding within higher level objects.

Encapsulation means that when we are going down the protocol stack and I'm going to move back up to the other end, we encapsulate data. What we're doing is we're taking information at a layer and we're sending it down the OSI model. At the packet is being encapsulated so information is taken, and it's taken to the next layer and it's sent along etc. For example, I'm going to add some information to a layer and then when it gets to the another layer I'm going to add the networking address, you know what where is it coming from where's it going to at the network and then the data link information and when I get down to another layer I'm going to give it what medium it's going to go on so by the time it gets down to this layer we have a full packet. The full packet gets put onto the medium whether it's wireless or wired. It gets sent along and when we get to the other end that full packet information comes. It gets de-encapsulated as it goes back up. It gets up to the application, let's say if it's a web browser or an email client.

For data access we have our network addresses (we have our source IP address, we have our destination IP address) that can either be an IPv4 or IPv6. The addresses ensures the delivery of the IP packet from the original source to the final destination either on the same network or the remote network. The data link addresses (you have the source data link address and you have the destination data link address) ensures the delivery of the data link frame from one network interface card or NIC [11] to another NIC card on the same network. Therefore, the difference between network addresses and data link addresses is that one sends it from one destination to the other on the same network or remote network and the data link addresses are on the same network.

III. Network Access

The data link layer protocol is made up of sub-layers. You have the logical link control (LLC) [52] which communicates with the network layer and then you have the Mac which defines the media access processes. The term MAC address [40] is “a bit of” the data link layer. Data link layer standards are Institute of Electrical and Electronics Engineers (IEEE), International Telecommunication Union (ITU), ISO and American National Standards Institute (ANSI). We saw some of these previously when discussing the Physical layer. Now media access control is when we control access to the media. But what does this mean? What we're really talking about is the topologies (physical topology and logical topology). Our physical topology is when we're saying what is the actual equipment. So, when you design your physical topology, you're laying your physical topology out. You are going to say I've got a server in a room; I've got a switch at a location and a router located elsewhere. It's going to show where everything is and it's going to label everything so you're going to know where physical equipment it is. Logical topology is the arrangement of devices on a computer network and how they communicate with one another. Logical topologies describe how signals act on the network. For example, you may have switch 1 (S1) but, on the diagram, we're listing out which connection it's tied to. We're giving our IP address [23]; we're saying this is on G0/0 (the link going out to the Internet). We're giving our IP address for that subnet. We're not giving out all the IP addresses we're just saying this is the subnet IP range.

The common physical LAN topologies are point-to-point, hub-and-spoke and mesh [37]. Point to Point topology is the simplest topology that connects two nodes directly together with a common link. A hub and spoke network is a traditional, proven, and widely used topology for all types of networks; it's also called the star topology. Essentially, the access point is physically connected to the Internet with a wire; like spokes on a wheel, all user devices connect to the wireless router in the center. A mesh topology can be a full mesh topology or a partially connected mesh topology. In a full mesh topology, every computer in the network has a connection to each of the other computers in that network. Mesh is more expensive to put into place because you have more wiring in place or you have more media connecting it but it has more redundancy to it. Two star networks connected gives a hybrid. Half duplex [38] of a communications system or computer circuit allows the transmission of signals in both directions but not simultaneously. Full-duplex [38] data transmission means that data can be transmitted in both directions on a signal carrier at the same time.

Carrier Sense Multiple Access or CSMA [71] is a Media Access Control (MAC) protocol that is used to control the flow of data in a transmission media so that packets do not get lost and data integrity is maintained. There are two modifications to CSMA, the CSMA CD (Collision Detection) [64] and CSMA CA (Collision Avoidance) [14], each having its own strengths. CSMA operates by sensing the state of the medium in order to prevent or recover from a collision. A collision happens when two transmitters transmit at the same time. The data gets scrambled, and the receivers would not be able to discern one from the other thereby causing the information to get lost. The lost information needs to be resent so that the receiver will get it. CSMA CD operates by detecting the occurrence of a collision. Once a collision is detected, CSMA CD immediately terminates the transmission so that the transmitter does not have to waste a lot of time in continuing. The last information can be retransmitted. In comparison, CSMA CA does not deal with the recovery after a collision. What it does is to check whether the medium is in use. If it is busy, then the transmitter waits until it is idle before it starts transmitting. This effectively minimizes the possibility of collisions and makes more efficient use of the medium. Another difference between CSMA CD and CSMA CA is where they are typically used. CSMA CD is used mostly in wired installations because it is possible to detect whether a collision has occurred. With wireless installations, it is not possible for the transmitter to detect whether a collision has occurred or not. That is why wireless installations often use CSMA CA instead of CSMA CD. Most people do not really have to deal with access control protocols as they work behind the scenes in order for our devices to work together. CSMA CD has also fallen out of favor with modern wired networks as they were only necessary with hubs and not with modern switches that route the information instead of broadcasting it.

Summary:

1. CSMA CD takes effect after a collision while CSMA CA takes effect before a collision.
2. CSMA CA reduces the possibility of a collision while CSMA CD only minimizes the recovery time.
3. CSMA CD is typically used in wired networks while CSMA CA is used in wireless networks.

A frame is a unit of communication in the data link layer. Data link layer takes the packets from the Network Layer and encapsulates them into frames. If the frame size becomes too large, then the packet may be divided into small sized frames. At receiver' end, data link layer picks up signals from hardware and assembles them into frames. Each frame type has three basic parts: Header, Data and Trailer. The structure of the data link layer frame may be specialized according to the type of protocol used. The frame structure used in two protocols: Point – to – Point Protocol (PPP) [65] and High-level Data Link Control (HDLC) [26] will be different.

We're going to be looking at the physical layer protocols we talked about protocols in previous slides as well as we're going to be talking about the physical layer protocols in these slides. We're going to be looking at Network media, the data link layer protocols and the media access control. Now we are going to identify types of network connections. When we talk about the physical layer connections, we're talking about how we transfer data from one end point to another end point or from an end point to another device. The different types of connections we have maybe a Cisco [77] wireless router or a home router. On the diagram of the router: Your Ethernet switch is where you can plug in your Ethernet cable. Your internet connection is where you put your LAN port. Your embedded wireless antenna doesn't actually pop up but some do. You can use wireless as well broadcast to a wireless card so the network interface card or you'll hear the term NIC. You can connect NICs in a lot of different ways. You can plug in an Ethernet cable to an RJ-45 connection [30] or you can use wireless routers. You can use also put our range extenders. This picks up the signal from the wire or from the router and then passes it on to devices so that if you're not getting a signal far enough you can put those in place.

The purpose of the physical layer is to accept a complete frame from the data link layer and encodes it (remember the encapsulation and de-encapsulation processes [21]. It encodes it as a series of signals that are transmitted onto the local media (it encapsulates the message and it sends it on the media). The digital signal consists of ones and zeroes. You can describe the physical layer media types by either Ethernet which is your copper or you can have fiber optics which is your light-emitting or you can have Bluetooth transmission or you can have wireless transmission through Wi-Fi and there's a few other ones too.

We have standards in place for physical layer. The standards organizations we talked about those in previous slides. Here we're talking about physical layer standards. You have those organizations that say if you're going to do a physical layer or standards in place that says they have to meet these certain specifications. E.g. Ethernet must have X amount of wires and it has to be a certain diameter and it has to be able to carry a certain amount of signal and so forth. These Standards are set forth in that physical layer characteristics. You have the functions of the physical layer, you have the physical components to it, you have encoding and signaling and the functions supporting the data transfer. The data transfer is impacted by the bandwidth. The term bandwidth means the capacity to a medium to carry data e.g. a highway or a road can fit a maximum of 2 or 8 lanes of cars. A small bandwidth might have a two-lane road with traffic going both ways and if you want to increase your bandwidth you add more lanes to that highway so you may have a six-lane highway where you have three lanes on each side or you have three lanes or six lanes of traffic that you can send data. Bandwidth is the "size" of the medium that you can transfer data through. Throughput is a little bit different. It is the measure of the transfer of bits across the media. Thus, bandwidth is how much capacity you have, while your throughput is the actual measure of the transfer of bits. The actual throughput of the data that's actually being sent through occurs over different types of physical media.

Copper cabling [47] is one of the most common physical media in networking. The reason it's so common is because it's inexpensive compared to other types of media. Fiber optics is expensive where Ethernet or copper cabling isn't expensive. Ethernet or copper cabling is inexpensive, it's easy to install, it's low resistance to electrical current, the distance and the signal interference is also a good. Characteristics of the copper cabling is that you have pretty good distance with it, and depending upon which category of Ethernet you have or which category of cabling you have it's going to go different differences based on whether it's a coax cable or an Ethernet. Different types of copper cabling are unshielded twisted-pair and shielded twisted-pair. Unshielded twisted-pair is less expensive as shielded twisted-pair uses some extra material (the shielding that goes over the wiring). Let's explore the reason for shielding. Let's say for example you're going to be putting in copper cabling and you've got to put it in next to some high-voltage lines or you're going to be putting it in next to some lights that are causing some interference. You're going to get some kind of electrical interference, so we have to put shielded twisted-pair in so the interference doesn't impact the data being sent to those copper cables. It's shielded so will cost you more. However, the unshielded cheaper but it's more susceptible to interference.

Unshielded twisted pair (UTP) cable [67] cancels out Electromagnetic interference (EMI) and Radio Frequency Interference (RFI) signals. You have different types of UTP cable: rollover, crossover and straight through. They are different depending upon how you put the wires through so depending on how the signals get sent through whether it's a rollover or crossover. You can also test you unshielded twisted-pair cable based on the cable pin outs. A device I can plug a point in and then I can use another little small cable that plugs in on the other end or I can plug both ends in and it will send a signal through the wire to tell me is it wired properly. This is the t568a and this is a t568b. The device is going to tell me whether I need a rollover a crossover or straight through. The device is going to tell me if I got that proper wiring done and did those signals get sent through which wires (wire one, two, three, four, five, six, seven, eight) and if is it correct on both ends.

Fiber-optic cabling allows you to transmit data over long distances. I mean much longer distances than regular unshielded twisted-pair Ethernet. It's flexible but the thin strands of glass can be broken so you must be careful when you handle it. It transmits with less attenuation which means it has less signal loss over a greater amount of distance and it's immune to EMI and RFI. It's immune to electromagnetic interference and radio frequency interference. If you do break a bundle of fiber optics cable it takes special tools to reconnect those back up. If you cut an Ethernet cable, it's easy just to take those pairs of wires and connect them back in. Fiber optics types include media single mode and multimode. You have fiber optic connectors that go on the end. Now we talk about UTP vs Fiber optics. Fiber optics is much more expensive to use so that's why you usually run fiber optics on longer distances or maybe between buildings. Thus, if you're connecting two local area networks together you may see fiber optics go between those buildings. You might see a city having fiber optics being put in and then when you get to the local building or the local area network is where you might use copper for the local area network. Bandwidth support from UTP is up to 10 gigabits, while on fiber optics it is from 10 megabits all the way up to a hundred gigabits. The distance is about 100 to 100,000 meters for fiber optics, while it's one to a hundred meters for UTP. UTP is very susceptible to EMI, RFI and electrical hazards, while fiber-optic side and it come completely immune to EMI, RFI and electrical hazards. However, the high cost, installation skills and safety precautions are impediments for fiber-optic usage.

Data communications over wireless media using radio or microwave frequencies passes distances which are much smaller or much shorter based upon what you're using that is, whether it's Bluetooth or Wi-Fi Bluetooth. Wi-Fi is over a much smaller range. There are different types of Wi-Fi e.g. we have Wi-Fi Bluetooth and WiMAX. There's some other ones out there too e.g. Wi-Fi-802.11a [19], Wi-Fi-802.11b [19], Wi-Fi-802.11g [19] and Wi-Fi-802.11n [6]. The first WLAN standard was created by the Institute of Electrical and Electronics Engineers in 1997. They called it 802.11 [32] after the group's name that was established to monitor its growth. Unfortunately, 802.11 only endorsed a maximum network bandwidth of 2 Mbps which was too slow for most applications. Therefore, 802.11 wireless products are no longer produced. However, from this original standard, a whole family has emerged. At home you may have a Wireless local area network and you might have a router. The router you may have set up and you have your you have your Wi-Fi come in to it. Then you broadcast out and your different devices pick up that signal and they can connect to the internet or your network based upon protocol set up. Thus, if you have Wi-Fi set up let's say on a mobile device and you can connect to the router and get signal and we call the router a wireless access point. A wireless access point allows you to broadcast messages out. There are also wireless NIC cards or Wireless NIC adapters. You can put a wireless NIC adapter on most laptops. However, before 2017 some older ones did not have NICs and you would have to plug those in using a wired connection for them to receive any network signal.

IV. Ethernet Protocol

We're going to talk about Ethernet protocol, we're going to look at the sub layers and the Ethernet

MAC address, we're going to look at LAN switches and we're going to look at address resolution protocol or ARP [5]. Ethernet encapsulation is when the ethernet operates in the data link layer and the physical layer. Ethernet supports data bandwidth from 10 megabits through 100 gigabits and Ethernet standards defined both the layer 2 protocols and the layer 1 protocols of the OSI model. The MAC sub-layer constitutes the lower sub layer of the data link layer and it's responsible for the data encapsulation and media access control. Ethernet has been evolving since its creation in 1973. Ethernet frame structure adds headers and trailers around the layer three PDU to encapsulate the message being sent. The minimum Ethernet frame size is 64 bytes and the maximum size is 1518 bytes. The frames frame smaller than the minimum or greater than the maximum are dropped. This is because anything smaller or greater could be the result of collisions or unwanted signals. A collision means you get data that hit each other and didn't come all the way through so you have an incomplete frame. If it's lower than 64 you know let's say if it's 61 bytes that's an invalid frame and if it's 1520 that's got extra signal information in there (there's ones and zeros in there that could be corrupt or not wrong information). Thus, the layer just drops those frames as well.

Your Ethernet Frame Fields include your preamble, your destination MAC address, your source MAC address, your Ether Type, your data and then your FCS field. The Ethernet MAC address or MAC addresses or media access control address is written in hexadecimal. It's 48 bits long and expressed as 12 hexadecimal digits. The vendor must use the assigned to the first three bytes so if you look at a machine address code or if you look at a MAC address you can look at the first three bytes and you can research that on the internet and you can find out who the vendor was of that of that that device. All MAC address is with the same OUI (Organizationally Unique Identifier) must be assigned a unique value in the last three bytes. When frames are processed the NIC card compares the destination MAC address in the frame with the device's physical MAC address stored in RAM. If there's a match that frame is passed up the OSI layer. If it doesn't match it passes it on, it discards that frame. It reads all the way up to the destination MAC and it then discards the rest, but it does read it partially. Thus, it does read all frames that come across that local area network. A representation of a MAC address: 00-50-2D-3B-07-BD. It can be represented with colons, dashes or dots and is case insensitive, so it doesn't matter if you capitalize B or C.

Let's talk about unicast broadcast and multicast. A unicast address is used when a frame is sent from a single transmitting device to a single destination device. It is one to one (1-1). A broadcast MAC address is used to address all nodes in a segment. The destination MAC address is the FF FFFFFFFF. It's a 48 1s in binary. It's one too many (1-M) or one too all (1-A). A multicast MAC address used to address groups of nodes in the segment or endpoints. The multicast MAC address is a special value that begins with the first six hex digits and within an IP range. It's one to some (1-S).

Let's switch gears to LAN switches so what are switches. They operate at the layer 2 of the OSI model. An Ethernet switch is a layer 2 device. A switch is a layer 2 device. Sometimes you have hybrids, you have hybrid routers and switches and so those are at layers 2 and 3, but we're just talking about just switches. At this point it uses the MAC address to make forwarding decisions. It does not need IP addressing because IP addressing (IPv4, IPv6) goes to the layer 3 of the OSI model. The MAC address table is sometimes referred to as a content addressable memory or CAM table. The switch will build a table, a MAC address table [48]. Now learning the MAC addresses. Switches dynamically build the CAM by monitoring source MACs. When you plug a device into a switch the switch will start broadcasting and saying who's out there, who is this connected too and the end device if it's set up properly will broadcast back and say hey I'm here, I'm a network interface card and here's my MAC address (and here's a base basic information). Thus, the switch builds a table so every frame that enters a switch is checked for new addresses and the frame is forwarded based on the CAM. The switch does really if you think about what the old-time telephone switch operators do. A person sitting there at a switchboard. They say. "ok who are you calling" and you say "well I'm calling number 0 0 1" and the operator says "ok well let me plug you into that person" and then the next person says "okay I'm calling 0 0 3" and the operator says "well I will plug you into 0 0 3." But you're not actually routing it outside the network because that's a router's job. You are keeping it internally on that local area network (LAN). Since the switch knows where to find specific MAC addresses it can filter frames to that port only. Filtering is not done if the destination MAC is not present in the CAM. Once the tables been built it can dynamically forward those frames, but it needs to build that table first to be able to do that.

Local Area Network (LAN) Switches [63] support different Switching Methods. Important Switching Methods are store and forward, cut-through and fragment-free. Switching Methods determine how a switch receives, processes, and forwards a Layer 2 Ethernet frame. Frame forwarding methods has store-and-forward and cut through switching. Cut through switching is a method for packet switching systems, wherein the switch starts forwarding a frame (or packet) before the whole frame has been received, normally as soon as the destination address is processed. It is fast forward switching, it's the lower lowest level of latency. Low latency and speed is obtained as it immediately forwards a packet after reading the destination address. In cut-through switching, the switch copies into its memory only the destination MAC address (first 6 bytes of the frame) of the frame before making a switching decision. A switch operating in cut-through switching mode reduces delay because the switch starts to forward the Ethernet frame as soon as it reads the destination MAC address and determines the outgoing switch port. Problem related with cut-through switching is that the switch may forward bad frames. Fragment-free (runtless switching) switching is an advanced form of cut-through switching. Fragment free switching switch stores the first 64 bytes of the frame before forwarding. The switches operating in cut-through switching read only up to the destination MAC address field in the Ethernet frame before making a switching decision. The switches operating in fragment-free switching read at least 64 bytes of the Ethernet frame before switching it to avoid forwarding Ethernet runt frames (Ethernet frames smaller than 64 bytes). In Store and Forward switching, Switch copies each complete Ethernet frame into the switch memory and computes a Cyclic Redundancy Check (CRC) [12]for errors. If a Cyclic Redundancy Check (CRC) error is found, the Ethernet frame is dropped and if there is no Cyclic Redundancy Check (CRC) error, the switch forwards the Ethernet frame to the destination device. Store and Forward switching can cause delay in switching since Cyclic Redundancy Check (CRC) is calculated for each Ethernet frame.

An Ethernet switch [35] may use a buffering technique to store and forward frames. Buffering may also be used when the destination port is busy. The area of memory where the switch stores the data is called the memory buffer. This memory buffer can use two methods for forwarding frames, port-based memory buffering and shared memory buffering. In port-based memory buffering frames are stored in queues that are linked to specific incoming ports. A frame is transmitted to the outgoing port only when all the frames ahead of it in the queue have been successfully transmitted. It is possible for a single frame to delay the transmission of all the frames in memory because of a busy destination port. This delay occurs even if the other frames could be transmitted to open destination ports. Shared memory buffering deposits all frames into a common memory buffer which all the ports on the switch share. The amount of buffer memory required by a port is dynamically allocated. The frames in the buffer are linked dynamically to the destination port. This allows the packet to be received on one port and then transmitted on another port, without moving it to a different queue. The switch keeps a map of frame to port links showing where a packet needs to be transmitted. The map link is cleared after the frame has been successfully transmitted. The memory buffer is shared. The number of frames stored in the buffer is restricted by the size of the entire memory buffer, and not limited to a single port buffer. This permits larger frames to be transmitted with fewer dropped frames. This is important to asymmetric switching, where frames are being exchanged between different rate ports.

Full duplex means that both ends of the connection can send and receive simultaneously. Half duplex means that only one into the connection can send at a time. Automatic medium-dependent interface crossover (Auto-MDIX) [80] is a feature that allows the switch interface to detect the required cable connection type (straight-through or crossover) and automatically configure the connection appropriately. Auto MDX detects the type of connection required and configures the interface accordingly. It helps reduce configuration errors. What happens is that the newer devices have Auto MDX on them will automatically detect and set its connection to full duplex if the other person is using this. Layer 2 addresses are used to move the frame within the local network. That's key to remember when we're at the layer 2, we're staying with inside the local area network. Layer 3 addresses are used to move the packets through remote networks which are outside your LAN. That's when it goes to the routing portion and gets routed somewhere else. A destination on the same network: physical addresses or MAC addresses are used for Ethernet NICs to Ethernet NIC communications on the same network. They communicate on the LAN without being routed and use layer 2 only. If you need to route outside of your LAN, you will go to your layer 3 and start to use IP addressing. ARP is address resolution protocol that is the combination of MAC and IP to facilitate to end-to-end communication. Address Resolution Protocol (ARP) is a procedure for mapping a dynamic Internet Protocol address (IP address) to a permanent physical machine address in a local area network (LAN). The physical machine address is also known as a Media Access Control or MAC address. The job of the ARP is essentially to translate 32-bit addresses to 48-bit addresses and vice-versa. This is necessary because in IP Version 4 (IPv4), the most common level of Internet Protocol (IP) in use today, an IP address is 32-bits long, but MAC addresses are 48-bits long. ARP works between network layers 2 and 3 of the Open Systems Interconnection model (OSI model). The MAC address exists on layer 2 of the OSI model, the data link layer, while the IP address exists on layer 3, the network layer. In IPv6, which uses 128-bit addresses, ARP has been replaced by the Neighbor Discovery protocol [51]. When a new computer joins a LAN, it is assigned a unique IP address to use for identification and communication. When an incoming packet destined for a host machine on a particular LAN arrives at a gateway, the gateway asks the ARP program to find a MAC address that matches the IP address. A table called the ARP cache maintains a record of each IP address and its corresponding MAC address. All operating systems in an IPv4 Ethernet network keep an ARP cache. Every time a host requests a MAC address in order to send a packet to another host in the LAN, it checks its ARP cache to see if the IP to MAC address translation already exists. If it does, then a new ARP request is unnecessary. If the translation does not already exist, then the request for network addresses is sent and ARP is performed. ARP broadcasts a request packet to all the machines on the LAN and asks if any of the machines know they are using that particular IP address. When a machine recognizes the IP address as its own, it sends a reply so ARP can update the cache for future reference and proceed with the communication.

V. Network Layer

We discuss the network layer protocols so we're doing the layer 3, we describe the purpose of the network IPv4 vs. IPv6 and we're going to take a look at routers. What is the network layer? The network layer is the layer 3 of the OSI model. In the previous sessions we looked at the physical and the data link layer. We looked at switches in previous session and how those worked. Well in this session we're going to look at the networking layer. The networking layer provides end-to-end transport processes. It addresses devices, it encapsulates, it routes and it de-encapsulates. The layer of protocols that we're going to talk about and use is the IPv4 and IPv6. In the case of the sender the layer 3 is going to encapsulate data, it's going to take the data and encapsulate it and send it down to the network stack. The network layer is going to encapsulate the information and say okay here's my IP address and so forth and then the layer 2 is going to put the MAC addressing information and it's going to send it down to the physical medium. Let's talk about the characteristics of the IP protocol. When we encapsulate the IP segments into IP packets for transmission the network layer adds a header so packets can be routed to the destination. If you have IP connectionless it means the sender doesn't know if the receiver is listening or whether the message arrived on time. The receiver doesn't know anything that is coming so when you hear IP connectionless you just mean that the sender is trying to send the information but with no guarantees. In some countries when you send a piece of mail to the Postal Service you just put a piece of mail in your mailbox. A postal worker picks it up that morning. The person receiving the mail may or may not know that they're getting a piece of mail. On the other end that mail just shows up so that's connectionless. But if you go to the post office and you say I want to send this piece of mail but I want a return receipt. This means when the main gets to the receiver the person that receives the piece of mail signs a piece of paper and says “yes” I've received this message/mail and then you get the message/mail back. This would be connection oriented. IP best effort delivery means there's no guarantees that a delivery is going to be made. Think about the time when you've tried to access a web site and you went you typed in the website address and it come back up and it said destination address unavailable. That's the “best effort” it just gives you what it can give you and that's it. It just says “I'm going to give you what I can and I'm not going to care about the rest.” The network layer is media independent so IP can travel over different types of media. It doesn't care if it's copper or if it's Wireless or fiber optics.

The IPv4 packet has been around a long time but it's being phased out. IPv6 is coming in because we ran out of IPv4 addresses. But IPv4 is going to be around for a long time. It is still very important. We now look at the IPv4 packet header and packet information. We have version, Internet header length, differentiated services, total length, identification, flag, fragment offset, time-to-live, header checksum, source IP address and destination IP address. The time-to-live means the packet will not hang out on the network forever. It's just going to say it's got so this got so long to live and if it doesn't get to its destination in an amount of time it just going to be destroyed. You don't want packets just floating around forever and gumming up everything. The IPv6 address space has improved packet handling and it eliminates the need for network address translation (NAT) [75]. You don't have to do NAT tables anymore which is nice because every device has an IPv6 address. Thus, encapsulating the IPv6 you have a simplified header format. There's no checksum process so it's more efficient. We have version, traffic class, flow label, payload length, next header, hop limit, source IP address and destination IP address. The 20-bit flow label field in the IPv6 header can be used by a source to label a set of packets belonging to the same flow. A flow is uniquely identified by the combination of the source address and of a non-zero Flow label. The purpose of flow label is to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. The flow label field makes routing more efficient. A Next Header field in the IPv6 header indicates the next extension header. Within each extension header is a Next Header field that indicates the next extension header. The last extension header indicates the upper layer protocol (such as TCP, UDP [76] (User Datagram Protocol), or ICMPv6 [18] (Internet Control Message Protocol, version 6)) contained within the upper layer protocol data unit. The 8-bit field also puts an upper limit on the maximum number of links between two IPv6 nodes. In this way, an IPv6 data packet is allowed a maximum of 255 hops before it is eventually discarded. An IPv6 data packet can pass through a maximum of 254 routers before being discarded. The 16-bit payload length field contains the length of the data field in octets/bits following the IPv6 packet header. The 16-bit Payload length field puts an upper limit on the maximum packet payload to 64 kilobytes. You have your source IP address and your destination IP address. We've looked at IPv4 and we've looked at IPv6 so now let's take a look at routing.

When we are leaving the local area network there needs to be a decision about the next hop. There's three types of destination. You can send it to yourself, the local host or remote host. The router reads the routing information it gets and says “I'm not going to do anything with this packet again” or “I will send it to a computer within my LAN” or “do I need to send it out to my remote host.” (via my remote connections). You can set up a default gateway. It's typically a router that goes outside the local area network. It routes traffic to other networks. It has a local IP address in the same address range as other hosts on the network. It's a gateway, it's a gatekeeper, it tells what goes in and out of the LAN. The host will use the default gateway when sending packets to remote host. You can use the netstat command netstat dash R to display the hosts routing table on a Windows machine and you would get the same thing on Linux. A router routing tables have a forwarding decision to make. Routers and host forward packets in a similar fashion. However, the main difference is that routers have more interfaces, while hosts have only one. Devices on a remote network are reached through a gateway. In the IPv4 routing table the router routing table stores information that the router knows about. You can use “show ip route” to display the routing table. The table also has information on how the route was learned, its trustworthiness and a rating on it. It also contains which interface to use to reach that specific destination. Directly connected routing table entries can be either C or an L. C identifies a directly connected network. It's automatically created when the interface is connected with an IP address and activated. L identifies if this is a local interface. This is the IPv4 address of the interface on the router.

We now look at remote network routing table entries. A remote destination can't be reached directly so packets have to be routed. Remote routes contain the addresses of the intermediate devices to be used to reach the destination. A router in a LAN knows nothing about the devices in another LAN. Thus for the two to communicate, the router in one LAN says “hey I've got a packet but I've got an ID” (let's just say that two end device are trying to communicate), the router says “ok well that's not on the local network so let me forward this onto my known destinations, and I'm going to forward it to this next router.” An intermediate router picks up the message and says “hey wait a minute I know that IP address, it's on my routing table and I'm going to forward it on internally.” (The IP is on the intermediate router’s LAN). Then the switch on the same LAN forwards it on through based on MAC addressing (that ARP table that we talked about in the previous sessions, where you have an ARP table and an IP address that are that are known). The next hop is among the series of routers that are connected together in a network and is the next possible destination for a data packet. More specifically, next hop is an IP address entry in a router's routing table, which specifies the next closest/most optimal router in its routing path.

The physical anatomy of a router. They have a CPU, they have memory, they have input/output devices, they use an operating system, they have power supplies, they have RAM built (your main RAM is built into the board), they have ROM and flash memory. They have lots of ports that support different types of connections. You have LAN and WAN interfaces. routers have LAN and WAN ports with LAN being local and WAN being white area. Different models ship with different ports depending upon the age. Ethernet it's a very common on different router models. When you're talking about the software the iOS image file is stored in the flash. Flash stores other system files and NVRAM [49] (Non-volatile random-access memory) stores configuration parameters. Your “startup-config” is in NVRAM. Random access memory is your running memory that gets that gets reset every time the device reboots. When you boot up the router says “ok I'm going to go to my flash, what image do I have? let me load that, do I need to load any other system files? then I'm going to go to NVRAM to pick up my configuration file and start running. In RAM I will now have my iOS [72] running, my running config and any changes I make. Remember you need to save those changes to your startup-config or the next time you reboot those changes won't work. You can also do a show version output to get the amounts of memory installed.

VI. Conclusion

The Media Layers of the open systems interconnection (OSI) reference model convert bits to packets. It is a very important aspect of network communication and consists of various networking protocols. At the lowest level the physical layer deals with Media, Signal and Binary Transmission of Bits. Then there is the Data Link layer which deals with media access control (MAC) and logical link control (LLC) Physical Addressing of Frames, for example Ethernet. Finally, there is the Network layer which deals with Path Determination and IP Logical addressing of Packets. This article gives a review of these Media Layers and will contribute to adding knowledge for a networking novice while consolidating concepts for an experienced professional or academic.

References Références Referencias

1. Acampora, Anthony S., and Mark J. Karol. "An overview of lightwave packet networks." IEEE Network 3, no. 1 (1989): 29-41.

2. Alfonsi, Benjamin. "I want my IPTV: Internet Protocol television predicted a winner." IEEE Distributed Systems Online 6, no. 2 (2005).
3. Alizadeh, Tooran, Tony H. Grubesic, and Edward Helderop. "Urban governance and big corporations in the digital economy: An investigation of socio-spatial implications of Google Fiber in Kansas City." Telematics and informatics 34, no. 7 (2017): 973-986.
4. Anton-Haro, Carles, and Mischa Dohler, eds. Machine-to-machine (M2M) communications: architecture, performance and applications. Elsevier, 2014.
5. Atkinson, R., and S. N. Bhatti. "Address resolution protocol (ARP) for the identifier-locator network protocol for IPv4 (ILNPv4)." RFC 6747, IRTF (2012).
6. Avila-Navarro, E., C. Cayuelas, and C. Reig. "Dual-band printed dipole antenna for Wi-Fi 802.11 n applications." Electronics letters 46, no. 21 (2010): 1421-1422.
7. Azzam, Albert A. High-speed cable modems: including IEEE 802.14 standards. McGraw-Hill Professional, 1997.
8. Bar-Noy, Amotz, Joseph SeffiNaor, and Baruch Schieber. "Pushing dependent data in clients–providers–servers systems." Wireless Networks 9, no. 5 (2003): 421-430.
9. Bektas, Filiz, Bojan Vondra, Peter E. Veith, Leopold Faltin, Alfred Pohl, and A. L. Scholtz. "Bluetooth communication employing antenna diversity." In Proceedings of the Eighth IEEE Symposium on Computers and Communications. ISCC 2003, pp. 652-657. IEEE, 2003.
10. Bell, Graham. "Different types of transmission lines used in communications: applications and uses. 1. Coaxial cable."
11. Bertozzi, Davide, Luca Benini, and Bruno Ricco. "Power aware network interface management for streaming multimedia." In 2002 IEEE Wireless Communications and Networking Conference Record. WCNC 2002 (Cat. No. 02TH8609), vol. 2, pp. 926-930. IEEE, 2002.
12. Borrelli, Chris. "IEEE 802.3 cyclic redundancy check." application note: Virtex Series and Virtex-II Family, XAPP209 (v1. 0) (2001).
13. Bruns, Ralf, Jürgen Dunkel, Henrik Masbruch, and Sebastian Stipkovic. "Intelligent M2M: Complex event processing for machine-to-machine communication." Expert Systems with Applications 42, no. 3 (2015): 1235-1246.
14. Chae, Chang-Joon, Elaine Wong, and Rodney S. Tucker. "Optical CSMA/CD media access scheme for Ethernet over passive optical network." IEEE Photonics Technology Letters 14, no. 5 (2002): 711-713.
15. Chan, Teresa, Nikita Joshi, Michelle Lin, and Neil Mehta. "Using Google Hangouts on Air for medical education: a disruptive way to leverage and facilitate remote communication and collaboration." Journal of graduate medical education 7, no. 2 (2015): 171-173.
16. Cho, Dong-Hoon, Jung-Hoon Song, Min-Su Kim, and Ki-Jun Han. "Performance analysis of the IEEE 802.16 wireless metropolitan area network." In First International Conference on Distributed Frameworks for Multimedia Applications, pp. 130-136. IEEE, 2005.
17. Cicconetti, Claudio, Luciano Lenzini, Enzo Mingozzi, and Carl Eklund. "Quality of service support in IEEE 802.16 networks." IEEE network 20, no. 2 (2006): 50-55.
18. Conta, Alex, Stephen Deering, and Mukesh Gupta. Internet control message protocol (icmpv6) for the internet protocol version 6 (ipv6) specification. RFC 2463, december, 1998.
19. De Carvalho, JAR Pacheco, H. Veiga, CF Ribeiro Pacheco, and A. D. Reis. "Extended performance research on Wi-Fi IEEE 802.11 a, b, g laboratory open point-to-multipoint and point-to-point links." In Transactions on Engineering Technologies, pp. 475-484. Springer, Singapore, 2016.
20. Dev, Roger H., Eric W. Gray, Eric S. Rustici, and Walter P. Scott. "Network management system using multifunction icons for information display." U.S. Patent 5,261,044, issued November 9, 1993.
21. Difrancisco, Michael, J. Stephenson, and C. Ellis. "Global Broadcast Service (GBS) end-to-end services: protocols and encapsulation." In MILCOM 2000 Proceedings. 21st Century Military Communications. Architectures and Technologies for Information Superiority (Cat. No. 00CH37155), vol. 2, pp. 704-709. IEEE, 2000.
22. Duchene, Julien, Colas Le Guernic, Eric Alata, Vincent Nicomette, and Mohamed Kaâniche. "State of the art of network protocol reverse engineering tools." Journal of Computer Virology and Hacking Techniques 14, no. 1 (2018): 53-68.
23. Egevang, Kjeld, and Paul Francis. The IP network address translator (NAT). RFC 1631, may, 1994.
24. Filibeli, M. Can, OznurOzkasap, and M. RehaCivanlar. "Embedded web server-based home appliance networks." Journal of Network and Computer Applications 30, no. 2 (2007): 499-514.
25. Forouzan, Behrouz A. TCP/IP protocol suite. McGraw-Hill, Inc., 2002.
26. Gelenbe, Erol, Jacques Labetoulle, and Guy Pujolle. "Performance evaluation of the HDLC protocol." Computer Networks (1976) 2, no. 4-5 (1978): 409-415.
27. Gien, Michel. "A file transfer protocol (FTP)." Computer Networks (1976) 2, no. 4-5 (1978): 312-319.

28. Goralski, Walter. The illustrated network: how TCP/IP works in a modern network. Morgan Kaufmann, 2017.
29. Groba, Christin, and Thomas Springer. "Exploring data forwarding with Bluetooth for participatory crowd monitoring." In 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp. 71-76. IEEE, 2019.
30. Han, Intark, Hong-Shik Park, Youn-KwaeJeong, and Kwang-Roh Park. "An integrated home server for communication, broadcast reception, and home automation." IEEE Transactions on Consumer Electronics 52, no. 1 (2006): 104-109.
31. Heires, Marcel. "The international organization for standardization (ISO)." New Political Economy 13, no. 3 (2008): 357-367.
32. Hiertz, Guido R., Dee Denteneer, Lothar Stibor, Yunpeng Zang, Xavier Pérez Costa, and Bernhard Walke. "The IEEE 802.11 universe." IEEE Communications Magazine 48, no. 1 (2010): 62-70.
33. Hinden, Robert, Stephen Deering, and Erik Nordmark. "IPv6 global unicast address format." Network Working Group Request for Comments 3587 (2003).
34. Hitz, Dave, James Lau, and Michael A. Malcolm. "File System Design for an NFS File Server Appliance." In USENIX winter, vol. 94. 1994.
35. Hoang, Hoai, Magnus Jonsson, UlrikHagstrom, and Anders Kallerdahl. "Switched real-time ethernet with earliest deadline first scheduling protocols and traffic handling." In Proceedings 16th International Parallel and Distributed Processing Symposium, pp. 6-pp. IEEE, 2001.
36. Kim, Ki Joon, and Dong-Hee Shin. "An acceptance model for smart watches." Internet Research (2015).
37. Knight, Paul, and Chris Lewis. "Layer 2 and 3 virtual private networks: taxonomy, technology, and standardization efforts." IEEE Communications Magazine 42, no. 6 (2004): 124-131.
38. Liu, Gang, Xianhao Chen, Zhiguo Ding, Zheng Ma, and F. Richard Yu. "Hybrid half-duplex/full-duplex cooperative non-orthogonal multiple access with transmit power adaptation." IEEE Transactions on Wireless Communications 17, no. 1 (2017): 506-519.
39. Liu, Ling. "Services computing: from cloud services, mobile services to internet of services." IEEE Transactions on Services Computing 5 (2016): 661-663.
40. Liu, Pei, Zhifeng Tao, and Shivendra Panwar. "A cooperative MAC protocol for wireless local area networks." In IEEE International Conference on Communications, 2005. ICC 2005. 2005, vol. 5, pp. 2962-2968. IEEE, 2005.
41. Mangold, Stefan, Sunghyun Choi, Peter May, Ole Klein, Guido Hiertz, and Lothar Stibor. "IEEE 802.11 e Wireless LAN for Quality of Service." In Proc. European Wireless, vol. 2, pp. 32-39. 2002.
42. Meng, Xiaoqiao, Zhiguo Xu, Beichuan Zhang, Geoff Huston, Songwu Lu, and Lixia Zhang. "IPv4 address allocation and the BGP routing table evolution." ACM SIGCOMM Computer Communication Review 35, no. 1 (2005): 71-80.
43. Messier, Andrew, Jared Robinson, and Kaveh Pahlavan. "Performance monitoring of a wireless campus area network." In Proceedings of 22nd Annual Conference on Local Computer Networks, pp. 232-238. IEEE, 1997.
44. Mirri, Silvia, Silvio Peroni, Paola Salomoni, Fabio Vitali, and VincenzoRubano. "Towards accessible graphs in HTML-based scientific articles." In 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), pp. 1067-1072. IEEE, 2017.
45. Na, Jun, and V. Rajaravivarma. "Multimedia file sharing in multimedia home or office business networks." In Proceedings of the 35th Southeastern Symposium on System Theory, 2003., pp. 237-241. IEEE, 2003.
46. Oda, Naoki, and Saneyasu Yamaguchi. "HTTP/2 performance evaluation with latency and packet losses." In 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), pp. 1-2. IEEE, 2018.
47. Oliviero, Andrew, and Bill Woodward. Cabling: the complete guide to copper and fiber-optic networking. John Wiley & Sons, 2014.
48. Pagiamtzis, Kostas, and Ali Sheikholeslami. "Content-addressable memory (CAM) circuits and architectures: A tutorial and survey." IEEE journal of solid-state circuits 41, no. 3 (2006): 712-727.
49. Pan, Liyang, Xian Luo, Yaru Yan, Jirong Ma, Dong Wu, and Jun Xu. "Pure logic CMOS based embedded non-volatile random access memory for low power RFID application." In 2008 IEEE Custom Integrated Circuits Conference, pp. 197-200. IEEE, 2008.
50. Pearce, Paul, Ben Jones, Frank Li, Roya Ensafi, Nick Feamster, Nick Weaver, and Vern Paxson. "Global Measurement of {DNS} Manipulation." In 26th {USENIX} Security Symposium ({USENIX} Security 17), pp. 307-323. 2017.
51. Pei, Guangyu, M. A. Albuquerque, Jae H. Kim, Douglas P. Nast, and Paul R. Norris. "A neighbor discovery protocol for directional antenna networks." In MILCOM 2005-2005 IEEE Military Communications Conference, pp. 487-492. IEEE, 2005.
52. Petras, Dietmar, and Andreas Hettich. "Performance Evaluation of a Logical Link Control Protocol for an ATM air interface." International Journal of Wireless Information Networks 4, no. 4 (1997): 225-232.

53. Popescu-Zeletin, Radu. "Implementing the ISO-OSI reference model." ACM SIGCOMM Computer Communication Review 13, no. 4 (1983): 56-66.
54. Popovic, Aleksandar, Ivan Lukovic, Vladimir Dimitrieski, and VerislavDjukic. "A DSL for modeling application-specific functionalities of business applications." Computer Languages, Systems & Structures 43 (2015): 69-95.
55. Powers, John P. Introduction to fiber optic systems. McGraw-Hill Professional, 1993.
56. Prasad, Neeli R. "IEEE 802.11 system design." In 2000 IEEE International Conference on Personal Wireless Communications. Conference Proceedings (Cat. No. 00TH8488), pp. 490-494. IEEE, 2000.
57. Pruet, Putjorn, Chee Siang Ang, and DeraviFarzin. "Understanding tablet computer usage among primary school students in underdeveloped areas: Students' technology experience, learning styles and attitudes." Computers in Human Behavior 55 (2016): 1131-1144.
58. Sagari, Shweta, Samuel Baysting, DolaSaha, Ivan Seskar, Wade Trappe, and Dipankar Raychaudhuri. "Coordinated dynamic spectrum management of LTE-U and Wi-Fi networks." In 2015 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), pp. 209-220. IEEE, 2015.
59. Santitoro, Ralph. "Metro Ethernet Services–A Technical Overview." In Metro Ethernet Forum, vol. 2006. 2003.
60. Sarker, Suprateek, and John D. Wells. "Understanding mobile handheld device use and adoption." Communications of the ACM 46, no. 12 (2003): 35-40.
61. Schatt, Stanley, and Stanley Schatt. Understanding local area networks. Sams, 1992.
62. Schollmeier, Rüdiger. "A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications." In Proceedings First International Conference on Peer-to-Peer Computing, pp. 101-102. IEEE, 2001.
63. Seifert, Rich. The switch book: the complete guide to LAN switching technology. John Wiley & Sons, Inc., 2000.
64. Sen, Souvik, Romit Roy Choudhury, and Srihari Nelakuditi. "CSMA/CN: Carrier sense multiple access with collision notification." IEEE/ACM Transactions on Networking 20, no. 2 (2011): 544-556.
65. Simpson, William, ed. RFC1661: the point-to-point protocol (PPP). RFC Editor, 1994.
66. Smith, Raymond, and Dennis Eaton. Wi-Fi Home Networking. McGraw-Hill, Inc., 2003.
67. Stephens, W. E., T. C. Banwell, G. R. Lalk, T. J. Robe, and K. C. Young. "Transmission of STS-3c (155 Mbit/sec) SONET/ATM signals over unshielded and shielded twisted pair copper wire." In [Conference Record] GLOBECOM' 92-Communications for Global Users: IEEE, pp. 170-174. IEEE, 1992.
68. Sunny, Albert, Sumankumar Panchal, Nikhil Vidhani, Subhashini Krishnasamy, S. V. R. Anand, Malati Hegde, Joy Kuri, and Anurag Kumar. "A generic controller for managing TCP transfers in IEEE 802.11 infrastructure WLANs." Journal of Network and Computer Applications 93 (2017): 13-26.
69. Thapliyal, Himanshu. "Internet of Things-based consumer electronics: reviewing existing consumer electronic devices, systems, and platforms and exploring new research paradigms." IEEE Consumer Electronics Magazine 7, no. 1 (2017): 66-67.
70. Tian, Hui, Jun Sun, Chin-Chen Chang, Yongfeng Huang, and Yonghong Chen. "Detecting bitrate modulation-based covert voice-over-IP communication." IEEE Communications Letters 22, no. 6 (2018): 1196-1199.
71. Tobagi, Fouad A., and V. Bruce Hunt. "Performance analysis of carrier sense multiple access with collision detection." Computer Networks (1976) 4, no. 5 (1980): 245-259.
72. Tracy, Kim W. "Mobile Application Development Experiences on Apple¿ s iOS and Android OS." Ieee Potentials 31, no. 4 (2012): 30-34.
73. Trogdon, Holly. "Lessons from google fiber: Why coordinated cost reductions to infrastructure access are necessary to achieve universal broadband deployment." Fed. Comm. LJ 66 (2013): 103.
74. Tse, David, and Pramod Viswanath. Fundamentals of wireless communication. Cambridge university press, 2005.
75. Tsirtsis, George, and PydaSrisuresh. "RFC2766: Network Address Translation-Protocol Translation (NAT-PT)." (2000).
76. UDP, User Datagram Protocol, and Datagram Sockets. "User Datagram Protocol." (1980).
77. Velte, Toby, and Anthony Velte. Cisco A Beginner's Guide. McGraw-Hill Education Group, 2013.
78. Vlosky, Richard P., Renée Fontenot, and Lydia Blalock. "Extranets: impacts on business practices and relationships." Journal of business & Industrial marketing (2000).
79. Werner, J-J. "The HDSL environment (high bit rate digital subscriber line)." IEEE Journal on selected areas in communications 9, no. 6 (1991): 785-800.
80. Yang, Kuo-pao, Theresa Beaubouef, and M. Chiu. "Lesson Learnt from Smart Home Automation Systems." Journal of Emerging Trends in Computing and Information Sciences 6, no. 3 (2015).
81. Zimmermann, Hubert. "OSI reference model-the ISO model of architecture for open systems interconnection." IEEE Transactions on communications 28, no. 4 (1980): 425-432.

Global Journals Guidelines Handbook 2020

www.GlobalJournals.org

Memberships

FELLOWS/ASSOCIATES OF COMPUTER SCIENCE RESEARCH COUNCIL

FCSRC/ACSRC MEMBERSHIPS

Introduction

FCSRC/ACSRC is the most prestigious membership of Global Journals accredited by Open Association of Research Society, U.S.A (OARS). The credentials of Fellow and Associate designations signify that the researcher has gained the knowledge of the fundamental and high-level concepts, and is a subject matter expert, proficient in an expertise course covering the professional code of conduct, and follows recognized standards of practice. The credentials are designated only to the researchers, scientists, and professionals that have been selected by a rigorous process by our Editorial Board and Management Board.

> Associates of FCSRC/ACSRC are scientists and researchers from around the world are working on projects/researches that have huge potentials. Members support Global Journals' mission to advance technology for humanity and the profession.

FCSRC

FELLOW OF COMPUTER SCIENCE RESEARCH COUNCIL

FELLOW OF COMPUTER SCIENCE RESEARCH COUNCIL is the most prestigious membership of Global Journals. It is an award and membership granted to individuals that the Open Association of Research Society judges to have made a 'substantial contribution to the improvement of computer science, technology, and electronics engineering.

> The primary objective is to recognize the leaders in research and scientific fields of the current era with a global perspective and to create a channel between them and other researchers for better exposure and knowledge sharing. Members are most eminent scientists, engineers, and technologists from all across the world. Fellows are elected for life through a peer review process on the basis of excellence in the respective domain. There is no limit on the number of new nominations made in any year. Each year, the Open Association of Research Society elect up to 12 new Fellow Members.

Benefit

To the institution

Get letter of appreciation

Global Journals sends a letter of appreciation of author to the Dean or CEO of the University or Company of which author is a part, signed by editor in chief or chief author.

Exclusive Network

Get access to a closed network

A FCSRC member gets access to a closed network of Tier 1 researchers and scientists with direct communication channel through our website. Fellows can reach out to other members or researchers directly.They should also be open to reaching out by other.

Career Credibility Exclusive Reputation

Certificate

Certificate, LoR and Laser-Momento

Fellows receive a printed copy of a certificate signed by our Chief Author that may be used for academic purposes and a personal recommendation letter to the dean of member's university.

Career Credibility Exclusive Reputation

Designation

Get honored title of membership

Fellows can use the honored title of membership. The “FCSRC” is an honored title which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., FCSRC or William Walldroff, M.S., FCSRC.

Career Credibility Exclusive Reputation

Recognition on the Platform

Better visibility and citation

All the Fellow members of FCSRC get a badge of "Leading Member of Global Journals" on the Research Community that distinguishes them from others. Additionally, the profile is also partially maintained by our team for better visibility and citation. All fellows get a dedicated page on the website with their biography.

Career Credibility Reputation

Future Work

Get discounts on the future publications

Fellows receive discounts on future publications with Global Journals up to 60%. Through our recommendation programs, members also receive discounts on publications made with OARS affiliated organizations.

Career Financial

GJ Account

Unlimited forward of Emails

Fellows get secure and fast GJ work emails with unlimited forward of emails that they may use them as their primary email. For example, john [AT] globaljournals [DOT] org.

Career Credibility Reputation

Premium Tools

Access to all the premium tools

To take future researches to the zenith, fellows receive access to all the premium tools that Global Journals have to offer along with the partnership with some of the best marketing leading tools out there.

Financial

Conferences & Events

Organize seminar/conference

Fellows are authorized to organize symposium/seminar/conference on behalf of Global Journal Incorporation (USA). They can also participate in the same organized by another institution as representative of Global Journal. In both the cases, it is mandatory for him to discuss with us and obtain our consent. Additionally, they get free research conferences (and others) alerts.

Career Credibility Financial

Early Invitations

Early invitations to all the symposiums, seminars, conferences

All fellows receive the early invitations to all the symposiums, seminars, conferences and webinars hosted by Global Journals in their subject.

Exclusive

Publishing Articles & Books

Earn 60% of sales proceeds

Fellows can publish articles (limited) without any fees. Also, they can earn up to 70% of sales proceeds from the sale of reference/review books/literature/publishing of research paper. The FCSRC member can decide its price and we can help in making the right decision.

Exclusive Financial

Reviewers

Get a remuneration of 15% of author fees

Fellow members are eligible to join as a paid peer reviewer at Global Journals Incorporation (USA) and can get a remuneration of 15% of author fees, taken from the author of a respective paper.

Financial

Access to Editorial Board

Become a member of the Editorial Board

Fellows may join as a member of the Editorial Board of Global Journals Incorporation (USA) after successful completion of three years as Fellow and as Peer Reviewer. Additionally, Fellows get a chance to nominate other members for Editorial Board.

Career Credibility Exclusive Reputation

And Much More

Get access to scientific museums and observatories across the globe

All members get access to 5 selected scientific museums and observatories across the globe. All researches published with Global Journals will be kept under deep archival facilities across regions for future protections and disaster recovery. They get 10 GB free secure cloud access for storing research files.

ACSRC

ASSOCIATE OF COMPUTER SCIENCE RESEARCH COUNCIL

ASSOCIATE OF COMPUTER SCIENCE RESEARCH COUNCIL is the membership of Global Journals awarded to individuals that the Open Association of Research Society judges to have made a 'substantial contribution to the improvement of computer science, technology, and electronics engineering.

> The primary objective is to recognize the leaders in research and scientific fields of the current era with a global perspective and to create a channel between them and other researchers for better exposure and knowledge sharing. Members are most eminent scientists, engineers, and technologists from all across the world. Associate membership can later be promoted to Fellow Membership. Associates are elected for life through a peer review process on the basis of excellence in the respective domain. There is no limit on the number of new nominations made in any year. Each year, the Open Association of Research Society elect up to 12 new Associate Members.

Benefit

To the institution

Get letter of appreciation

Global Journals sends a letter of appreciation of author to the Dean or CEO of the University or Company of which author is a part, signed by editor in chief or chief author.

Exclusive Network

Get access to a closed network

A ACSRC member gets access to a closed network of Tier 2 researchers and scientists with direct communication channel through our website. Associates can reach out to other members or researchers directly.They should also be open to reaching out by other.

Career | Credibility | Exclusive | Reputation

Certificate

Certificate, LoR and Laser-Momento

Associates receive a printed copy of a certificate signed by our Chief Author that may be used for academic purposes and a personal recommendation letter to the dean of member's university.

Career | Credibility | Exclusive | Reputation

Designation

Get honored title of membership

Associates can use the honored title of membership. The “ACSRC” is an honored title which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., ACSRC or William Walldroff, M.S., ACSRC.

Career | Credibility | Exclusive | Reputation

Recognition on the Platform

Better visibility and citation

All the Associate members of ACSRC get a badge of "Leading Member of Global Journals" on the Research Community that distinguishes them from others. Additionally, the profile is also partially maintained by our team for better visibility and citation.

Career | Credibility | Reputation

Future Work

Get discounts on the future publications

Associates receive discounts on future publications with Global Journals up to 30%. Through our recommendation programs, members also receive discounts on publications made with OARS affiliated organizations.

Career Financial

GJ Account

Unlimited forward of Emails

Associates get secure and fast GJ work emails with 5GB forward of emails that they may use them as their primary email. For example, john [AT] globaljournals [DOT] org.

Career Credibility Reputation

Premium Tools

Access to all the premium tools

To take future researches to the zenith, associates receive access to all the premium tools that Global Journals have to offer along with the partnership with some of the best marketing leading tools out there.

Financial

Conferences & Events

Organize seminar/conference

Associates are authorized to organize symposium/seminar/conference on behalf of Global Journal Incorporation (USA). They can also participate in the same organized by another institution as representative of Global Journal. In both the cases, it is mandatory for him to discuss with us and obtain our consent. Additionally, they get free research conferences (and others) alerts.

Career Credibility Financial

Early Invitations

Early invitations to all the symposiums, seminars, conferences

All associates receive the early invitations to all the symposiums, seminars, conferences and webinars hosted by Global Journals in their subject.

Exclusive

Publishing Articles & Books

Earn 30-40% of sales proceeds

Associates can publish articles (limited) without any fees. Also, they can earn up to 30-40% of sales proceeds from the sale of reference/review books/literature/publishing of research paper.

Exclusive Financial

Reviewers

Get a remuneration of 15% of author fees

Associate members are eligible to join as a paid peer reviewer at Global Journals Incorporation (USA) and can get a remuneration of 15% of author fees, taken from the author of a respective paper.

Financial

And Much More

Get access to scientific museums and observatories across the globe

All members get access to 2 selected scientific museums and observatories across the globe. All researches published with Global Journals will be kept under deep archival facilities across regions for future protections and disaster recovery. They get 5 GB free secure cloud access for storing research files.

ASSOCIATE	FELLOW	RESEARCH GROUP	BASIC
$4800	$6800	$12500.00	APC
lifetime designation	lifetime designation	organizational	per article
Certificate, LoR and Momento 2 discounted publishing/year **Gradation** of Research 10 research contacts/day 1 **GB** Cloud Storage **GJ** Community Access	**Certificate,** LoR and Momento **Unlimited** discounted publishing/year **Gradation** of Research **Unlimited** research contacts/day 5 **GB** Cloud Storage **Online Presense** Assistance **GJ** Community Access	**Certificates,** LoRs and Momentos **Unlimited** free publishing/year **Gradation** of Research **Unlimited** research contacts/day **Unlimited** Cloud Storage **Online Presense** Assistance **GJ** Community Access	**GJ** Community Access

Preferred Author Guidelines

We accept the manuscript submissions in any standard (generic) format.

We typeset manuscripts using advanced typesetting tools like Adobe In Design, CorelDraw, TeXnicCenter, and TeXStudio. We usually recommend authors submit their research using any standard format they are comfortable with, and let Global Journals do the rest.

Alternatively, you can download our basic template from https://globaljournals.org/Template.zip

Authors should submit their complete paper/article, including text illustrations, graphics, conclusions, artwork, and tables. Authors who are not able to submit manuscript using the form above can email the manuscript department at submit@globaljournals.org or get in touch with chiefeditor@globaljournals.org if they wish to send the abstract before submission.

Before and during Submission

Authors must ensure the information provided during the submission of a paper is authentic. Please go through the following checklist before submitting:

1. Authors must go through the complete author guideline and understand and *agree to Global Journals' ethics and code of conduct,* along with author responsibilities.
2. Authors must accept the privacy policy, terms, and conditions of Global Journals.
3. Ensure corresponding author’s email address and postal address are accurate and reachable.
4. Manuscript to be submitted must include keywords, an abstract, a paper title, co-author(s') names and details (email address, name, phone number, and institution), figures and illustrations in vector format including appropriate captions, tables, including titles and footnotes, a conclusion, results, acknowledgments and references.
5. Authors should submit paper in a ZIP archive if any supplementary files are required along with the paper.
6. Proper permissions must be acquired for the use of any copyrighted material.
7. Manuscript submitted *must not have been submitted or published elsewhere* and all authors must be aware of the submission.

Declaration of Conflicts of Interest

It is required for authors to declare all financial, institutional, and personal relationships with other individuals and organizations that could influence (bias) their research.

Policy on Plagiarism

Plagiarism is not acceptable in Global Journals submissions at all.

Plagiarized content will not be considered for publication. We reserve the right to inform authors’ institutions about plagiarism detected either before or after publication. If plagiarism is identified, we will follow COPE guidelines:

Authors are solely responsible for all the plagiarism that is found. The author must not fabricate, falsify or plagiarize existing research data. The following, if copied, will be considered plagiarism:

- Words (language)
- Ideas
- Findings
- Writings
- Diagrams
- Graphs
- Illustrations
- Lectures

- Printed material
- Graphic representations
- Computer programs
- Electronic material
- Any other original work

Authorship Policies

Global Journals follows the definition of authorship set up by the Open Association of Research Society, USA. According to its guidelines, authorship criteria must be based on:

1. Substantial contributions to the conception and acquisition of data, analysis, and interpretation of findings.
2. Drafting the paper and revising it critically regarding important academic content.
3. Final approval of the version of the paper to be published.

Changes in Authorship

The corresponding author should mention the name and complete details of all co-authors during submission and in manuscript. We support addition, rearrangement, manipulation, and deletions in authors list till the early view publication of the journal. We expect that corresponding author will notify all co-authors of submission. We follow COPE guidelines for changes in authorship.

Copyright

During submission of the manuscript, the author is confirming an exclusive license agreement with Global Journals which gives Global Journals the authority to reproduce, reuse, and republish authors' research. We also believe in flexible copyright terms where copyright may remain with authors/employers/institutions as well. Contact your editor after acceptance to choose your copyright policy. You may follow this form for copyright transfers.

Appealing Decisions

Unless specified in the notification, the Editorial Board's decision on publication of the paper is final and cannot be appealed before making the major change in the manuscript.

Acknowledgments

Contributors to the research other than authors credited should be mentioned in Acknowledgments. The source of funding for the research can be included. Suppliers of resources may be mentioned along with their addresses.

Declaration of funding sources

Global Journals is in partnership with various universities, laboratories, and other institutions worldwide in the research domain. Authors are requested to disclose their source of funding during every stage of their research, such as making analysis, performing laboratory operations, computing data, and using institutional resources, from writing an article to its submission. This will also help authors to get reimbursements by requesting an open access publication letter from Global Journals and submitting to the respective funding source.

Preparing your Manuscript

Authors can submit papers and articles in an acceptable file format: MS Word (doc, docx), LaTeX (.tex, .zip or .rar including all of your files), Adobe PDF (.pdf), rich text format (.rtf), simple text document (.txt), Open Document Text (.odt), and Apple Pages (.pages). Our professional layout editors will format the entire paper according to our official guidelines. This is one of the highlights of publishing with Global Journals—authors should not be concerned about the formatting of their paper. Global Journals accepts articles and manuscripts in every major language, be it Spanish, Chinese, Japanese, Portuguese, Russian, French, German, Dutch, Italian, Greek, or any other national language, but the title, subtitle, and abstract should be in English. This will facilitate indexing and the pre-peer review process.

The following is the official style and template developed for publication of a research paper. Authors are not required to follow this style during the submission of the paper. It is just for reference purposes.

Manuscript Style Instruction (Optional)

- Microsoft Word Document Setting Instructions.
- Font type of all text should be Swis721 Lt BT.
- Page size: 8.27" x 11'", left margin: 0.65, right margin: 0.65, bottom margin: 0.75.
- Paper title should be in one column of font size 24.
- Author name in font size of 11 in one column.
- Abstract: font size 9 with the word "Abstract" in bold italics.
- Main text: font size 10 with two justified columns.
- Two columns with equal column width of 3.38 and spacing of 0.2.
- First character must be three lines drop-capped.
- The paragraph before spacing of 1 pt and after of 0 pt.
- Line spacing of 1 pt.
- Large images must be in one column.
- The names of first main headings (Heading 1) must be in Roman font, capital letters, and font size of 10.
- The names of second main headings (Heading 2) must not include numbers and must be in italics with a font size of 10.

Structure and Format of Manuscript

The recommended size of an original research paper is under 15,000 words and review papers under 7,000 words. Research articles should be less than 10,000 words. Research papers are usually longer than review papers. Review papers are reports of significant research (typically less than 7,000 words, including tables, figures, and references)

A research paper must include:

a) A title which should be relevant to the theme of the paper.
b) A summary, known as an abstract (less than 150 words), containing the major results and conclusions.
c) Up to 10 keywords that precisely identify the paper's subject, purpose, and focus.
d) An introduction, giving fundamental background objectives.
e) Resources and techniques with sufficient complete experimental details (wherever possible by reference) to permit repetition, sources of information must be given, and numerical methods must be specified by reference.
f) Results which should be presented concisely by well-designed tables and figures.
g) Suitable statistical data should also be given.
h) All data must have been gathered with attention to numerical detail in the planning stage.

Design has been recognized to be essential to experiments for a considerable time, and the editor has decided that any paper that appears not to have adequate numerical treatments of the data will be returned unrefereed.

i) Discussion should cover implications and consequences and not just recapitulate the results; conclusions should also be summarized.
j) There should be brief acknowledgments.
k) There ought to be references in the conventional format. Global Journals recommends APA format.

Authors should carefully consider the preparation of papers to ensure that they communicate effectively. Papers are much more likely to be accepted if they are carefully designed and laid out, contain few or no errors, are summarizing, and follow instructions. They will also be published with much fewer delays than those that require much technical and editorial correction.

The Editorial Board reserves the right to make literary corrections and suggestions to improve brevity.

Format Structure

It is necessary that authors take care in submitting a manuscript that is written in simple language and adheres to published guidelines.

All manuscripts submitted to Global Journals should include:

Title

The title page must carry an informative title that reflects the content, a running title (less than 45 characters together with spaces), names of the authors and co-authors, and the place(s) where the work was carried out.

Author details

The full postal address of any related author(s) must be specified.

Abstract

The abstract is the foundation of the research paper. It should be clear and concise and must contain the objective of the paper and inferences drawn. It is advised to not include big mathematical equations or complicated jargon.

Many researchers searching for information online will use search engines such as Google, Yahoo or others. By optimizing your paper for search engines, you will amplify the chance of someone finding it. In turn, this will make it more likely to be viewed and cited in further works. Global Journals has compiled these guidelines to facilitate you to maximize the web-friendliness of the most public part of your paper.

Keywords

A major lynchpin of research work for the writing of research papers is the keyword search, which one will employ to find both library and internet resources. Up to eleven keywords or very brief phrases have to be given to help data retrieval, mining, and indexing.

One must be persistent and creative in using keywords. An effective keyword search requires a strategy: planning of a list of possible keywords and phrases to try.

Choice of the main keywords is the first tool of writing a research paper. Research paper writing is an art. Keyword search should be as strategic as possible.

One should start brainstorming lists of potential keywords before even beginning searching. Think about the most important concepts related to research work. Ask, "What words would a source have to include to be truly valuable in a research paper?" Then consider synonyms for the important words.

It may take the discovery of only one important paper to steer in the right keyword direction because, in most databases, the keywords under which a research paper is abstracted are listed with the paper.

Numerical Methods

Numerical methods used should be transparent and, where appropriate, supported by references.

Abbreviations

Authors must list all the abbreviations used in the paper at the end of the paper or in a separate table before using them.

Formulas and equations

Authors are advised to submit any mathematical equation using either MathJax, KaTeX, or LaTeX, or in a very high-quality image.

Tables, Figures, and Figure Legends

Tables: Tables should be cautiously designed, uncrowned, and include only essential data. Each must have an Arabic number, e.g., Table 4, a self-explanatory caption, and be on a separate sheet. Authors must submit tables in an editable format and not as images. References to these tables (if any) must be mentioned accurately.

Figures

Figures are supposed to be submitted as separate files. Always include a citation in the text for each figure using Arabic numbers, e.g., Fig. 4. Artwork must be submitted online in vector electronic form or by emailing it.

Preparation of Eletronic Figures for Publication

Although low-quality images are sufficient for review purposes, print publication requires high-quality images to prevent the final product being blurred or fuzzy. Submit (possibly by e-mail) EPS (line art) or TIFF (halftone/ photographs) files only. MS PowerPoint and Word Graphics are unsuitable for printed pictures. Avoid using pixel-oriented software. Scans (TIFF only) should have a resolution of at least 350 dpi (halftone) or 700 to 1100 dpi (line drawings). Please give the data for figures in black and white or submit a Color Work Agreement form. EPS files must be saved with fonts embedded (and with a TIFF preview, if possible).

For scanned images, the scanning resolution at final image size ought to be as follows to ensure good reproduction: line art: >650 dpi; halftones (including gel photographs): >350 dpi; figures containing both halftone and line images: >650 dpi.

Color charges: Authors are advised to pay the full cost for the reproduction of their color artwork. Hence, please note that if there is color artwork in your manuscript when it is accepted for publication, we would require you to complete and return a Color Work Agreement form before your paper can be published. Also, you can email your editor to remove the color fee after acceptance of the paper.

Tips for writing a good quality Computer Science Research Paper

Techniques for writing a good quality computer science research paper:

1. Choosing the topic: In most cases, the topic is selected by the interests of the author, but it can also be suggested by the guides. You can have several topics, and then judge which you are most comfortable with. This may be done by asking several questions of yourself, like "Will I be able to carry out a search in this area? Will I find all necessary resources to accomplish the search? Will I be able to find all information in this field area?" If the answer to this type of question is "yes," then you ought to choose that topic. In most cases, you may have to conduct surveys and visit several places. Also, you might have to do a lot of work to find all the rises and falls of the various data on that subject. Sometimes, detailed information plays a vital role, instead of short information. Evaluators are human: The first thing to remember is that evaluators are also human beings. They are not only meant for rejecting a paper. They are here to evaluate your paper. So present your best aspect.

2. Think like evaluators: If you are in confusion or getting demotivated because your paper may not be accepted by the evaluators, then think, and try to evaluate your paper like an evaluator. Try to understand what an evaluator wants in your research paper, and you will automatically have your answer. Make blueprints of paper: The outline is the plan or framework that will help you to arrange your thoughts. It will make your paper logical. But remember that all points of your outline must be related to the topic you have chosen.

3. Ask your guides: If you are having any difficulty with your research, then do not hesitate to share your difficulty with your guide (if you have one). They will surely help you out and resolve your doubts. If you can't clarify what exactly you require for your work, then ask your supervisor to help you with an alternative. He or she might also provide you with a list of essential readings.

4. Use of computer is recommended: As you are doing research in the field of computer science then this point is quite obvious. Use right software: Always use good quality software packages. If you are not capable of judging good software, then you can lose the quality of your paper unknowingly. There are various programs available to help you which you can get through the internet.

5. Use the internet for help: An excellent start for your paper is using Google. It is a wondrous search engine, where you can have your doubts resolved. You may also read some answers for the frequent question of how to write your research paper or find a model research paper. You can download books from the internet. If you have all the required books, place importance on reading, selecting, and analyzing the specified information. Then sketch out your research paper. Use big pictures: You may use encyclopedias like Wikipedia to get pictures with the best resolution. At Global Journals, you should strictly follow here.

6. Bookmarks are useful: When you read any book or magazine, you generally use bookmarks, right? It is a good habit which helps to not lose your continuity. You should always use bookmarks while searching on the internet also, which will make your search easier.

7. Revise what you wrote: When you write anything, always read it, summarize it, and then finalize it.

8. Make every effort: Make every effort to mention what you are going to write in your paper. That means always have a good start. Try to mention everything in the introduction—what is the need for a particular research paper. Polish your work with good writing skills and always give an evaluator what he wants. Make backups: When you are going to do any important thing like making a research paper, you should always have backup copies of it either on your computer or on paper. This protects you from losing any portion of your important data.

9. Produce good diagrams of your own: Always try to include good charts or diagrams in your paper to improve quality. Using several unnecessary diagrams will degrade the quality of your paper by creating a hodgepodge. So always try to include diagrams which were made by you to improve the readability of your paper. Use of direct quotes: When you do research relevant to literature, history, or current affairs, then use of quotes becomes essential, but if the study is relevant to science, use of quotes is not preferable.

10.Use proper verb tense: Use proper verb tenses in your paper. Use past tense to present those events that have happened. Use present tense to indicate events that are going on. Use future tense to indicate events that will happen in the future. Use of wrong tenses will confuse the evaluator. Avoid sentences that are incomplete.

11. Pick a good study spot: Always try to pick a spot for your research which is quiet. Not every spot is good for studying.

12. Know what you know: Always try to know what you know by making objectives, otherwise you will be confused and unable to achieve your target.

13. Use good grammar: Always use good grammar and words that will have a positive impact on the evaluator; use of good vocabulary does not mean using tough words which the evaluator has to find in a dictionary. Do not fragment sentences. Eliminate one-word sentences. Do not ever use a big word when a smaller one would suffice.

Verbs have to be in agreement with their subjects. In a research paper, do not start sentences with conjunctions or finish them with prepositions. When writing formally, it is advisable to never split an infinitive because someone will (wrongly) complain. Avoid clichés like a disease. Always shun irritating alliteration. Use language which is simple and straightforward. Put together a neat summary.

14. Arrangement of information: Each section of the main body should start with an opening sentence, and there should be a changeover at the end of the section. Give only valid and powerful arguments for your topic. You may also maintain your arguments with records.

15. Never start at the last minute: Always allow enough time for research work. Leaving everything to the last minute will degrade your paper and spoil your work.

16. Multitasking in research is not good: Doing several things at the same time is a bad habit in the case of research activity. Research is an area where everything has a particular time slot. Divide your research work into parts, and do a particular part in a particular time slot.

17. Never copy others' work: Never copy others' work and give it your name because if the evaluator has seen it anywhere, you will be in trouble. Take proper rest and food: No matter how many hours you spend on your research activity, if you are not taking care of your health, then all your efforts will have been in vain. For quality research, take proper rest and food.

18. Go to seminars: Attend seminars if the topic is relevant to your research area. Utilize all your resources.

19. Refresh your mind after intervals: Try to give your mind a rest by listening to soft music or sleeping in intervals. This will also improve your memory. Acquire colleagues: Always try to acquire colleagues. No matter how sharp you are, if you acquire colleagues, they can give you ideas which will be helpful to your research.

20. Think technically: Always think technically. If anything happens, search for its reasons, benefits, and demerits. Think and then print: When you go to print your paper, check that tables are not split, headings are not detached from their descriptions, and page sequence is maintained.

21. Adding unnecessary information: Do not add unnecessary information like "I have used MS Excel to draw graphs." Irrelevant and inappropriate material is superfluous. Foreign terminology and phrases are not apropos. One should never take a broad view. Analogy is like feathers on a snake. Use words properly, regardless of how others use them. Remove quotations. Puns are for kids, not grunt readers. Never oversimplify: When adding material to your research paper, never go for oversimplification; this will definitely irritate the evaluator. Be specific. Never use rhythmic redundancies. Contractions shouldn't be used in a research paper. Comparisons are as terrible as clichés. Give up ampersands, abbreviations, and so on. Remove commas that are not necessary. Parenthetical words should be between brackets or commas. Understatement is always the best way to put forward earth-shaking thoughts. Give a detailed literary review.

22. Report concluded results: Use concluded results. From raw data, filter the results, and then conclude your studies based on measurements and observations taken. An appropriate number of decimal places should be used. Parenthetical remarks are prohibited here. Proofread carefully at the final stage. At the end, give an outline to your arguments. Spot perspectives of further study of the subject. Justify your conclusion at the bottom sufficiently, which will probably include examples.

23. Upon conclusion: Once you have concluded your research, the next most important step is to present your findings. Presentation is extremely important as it is the definite medium though which your research is going to be in print for the rest of the crowd. Care should be taken to categorize your thoughts well and present them in a logical and neat manner. A good quality research paper format is essential because it serves to highlight your research paper and bring to light all necessary aspects of your research.

Informal Guidelines of Research Paper Writing

Key points to remember:

- Submit all work in its final form.
- Write your paper in the form which is presented in the guidelines using the template.
- Please note the criteria peer reviewers will use for grading the final paper.

Final points:

One purpose of organizing a research paper is to let people interpret your efforts selectively. The journal requires the following sections, submitted in the order listed, with each section starting on a new page:

The introduction: This will be compiled from reference matter and reflect the design processes or outline of basis that directed you to make a study. As you carry out the process of study, the method and process section will be constructed like that. The results segment will show related statistics in nearly sequential order and direct reviewers to similar intellectual paths throughout the data that you gathered to carry out your study.

The discussion section:

This will provide understanding of the data and projections as to the implications of the results. The use of good quality references throughout the paper will give the effort trustworthiness by representing an alertness to prior workings.

Writing a research paper is not an easy job, no matter how trouble-free the actual research or concept. Practice, excellent preparation, and controlled record-keeping are the only means to make straightforward progression.

General style:

Specific editorial column necessities for compliance of a manuscript will always take over from directions in these general guidelines.

To make a paper clear: Adhere to recommended page limits.

Mistakes to avoid:

- Insertion of a title at the foot of a page with subsequent text on the next page.
- Separating a table, chart, or figure—confine each to a single page.
- Submitting a manuscript with pages out of sequence.
- In every section of your document, use standard writing style, including articles ("a" and "the").
- Keep paying attention to the topic of the paper.
- Use paragraphs to split each significant point (excluding the abstract).
- Align the primary line of each section.
- Present your points in sound order.
- Use present tense to report well-accepted matters.
- Use past tense to describe specific results.
- Do not use familiar wording; don't address the reviewer directly. Don't use slang or superlatives.
- Avoid use of extra pictures—include only those figures essential to presenting results.

Title page:

Choose a revealing title. It should be short and include the name(s) and address(es) of all authors. It should not have acronyms or abbreviations or exceed two printed lines.

Abstract: This summary should be two hundred words or less. It should clearly and briefly explain the key findings reported in the manuscript and must have precise statistics. It should not have acronyms or abbreviations. It should be logical in itself. Do not cite references at this point.

An abstract is a brief, distinct paragraph summary of finished work or work in development. In a minute or less, a reviewer can be taught the foundation behind the study, common approaches to the problem, relevant results, and significant conclusions or new questions.

Write your summary when your paper is completed because how can you write the summary of anything which is not yet written? Wealth of terminology is very essential in abstract. Use comprehensive sentences, and do not sacrifice readability for brevity; you can maintain it succinctly by phrasing sentences so that they provide more than a lone rationale. The author can at this moment go straight to shortening the outcome. Sum up the study with the subsequent elements in any summary. Try to limit the initial two items to no more than one line each.

Reason for writing the article—theory, overall issue, purpose.

- Fundamental goal.
- To-the-point depiction of the research.
- Consequences, including definite statistics—if the consequences are quantitative in nature, account for this; results of any numerical analysis should be reported. Significant conclusions or questions that emerge from the research.

Approach:

- Single section and succinct.
- An outline of the job done is always written in past tense.
- Concentrate on shortening results—limit background information to a verdict or two.
- Exact spelling, clarity of sentences and phrases, and appropriate reporting of quantities (proper units, important statistics) are just as significant in an abstract as they are anywhere else.

Introduction:

The introduction should "introduce" the manuscript. The reviewer should be presented with sufficient background information to be capable of comprehending and calculating the purpose of your study without having to refer to other works. The basis for the study should be offered. Give the most important references, but avoid making a comprehensive appraisal of the topic. Describe the problem visibly. If the problem is not acknowledged in a logical, reasonable way, the reviewer will give no attention to your results. Speak in common terms about techniques used to explain the problem, if needed, but do not present any particulars about the protocols here.

The following approach can create a valuable beginning:

- Explain the value (significance) of the study.
- Defend the model—why did you employ this particular system or method? What is its compensation? Remark upon its appropriateness from an abstract point of view as well as pointing out sensible reasons for using it.
- Present a justification. State your particular theory(-ies) or aim(s), and describe the logic that led you to choose them.
- Briefly explain the study's tentative purpose and how it meets the declared objectives.

Approach:

Use past tense except for when referring to recognized facts. After all, the manuscript will be submitted after the entire job is done. Sort out your thoughts; manufacture one key point for every section. If you make the four points listed above, you will need at least four paragraphs. Present surrounding information only when it is necessary to support a situation. The reviewer does not desire to read everything you know about a topic. Shape the theory specifically—do not take a broad view.

As always, give awareness to spelling, simplicity, and correctness of sentences and phrases.

Procedures (methods and materials):

This part is supposed to be the easiest to carve if you have good skills. A soundly written procedures segment allows a capable scientist to replicate your results. Present precise information about your supplies. The suppliers and clarity of reagents can be helpful bits of information. Present methods in sequential order, but linked methodologies can be grouped as a segment. Be concise when relating the protocols. Attempt to give the least amount of information that would permit another capable scientist to replicate your outcome, but be cautious that vital information is integrated. The use of subheadings is suggested and ought to be synchronized with the results section.

When a technique is used that has been well-described in another section, mention the specific item describing the way, but draw the basic principle while stating the situation. The purpose is to show all particular resources and broad procedures so that another person may use some or all of the methods in one more study or referee the scientific value of your work. It is not to be a step-by-step report of the whole thing you did, nor is a methods section a set of orders.

Materials:

Materials may be reported in part of a section or else they may be recognized along with your measures.

Methods:

- Report the method and not the particulars of each process that engaged the same methodology.
- Describe the method entirely.
- To be succinct, present methods under headings dedicated to specific dealings or groups of measures.
- Simplify—detail how procedures were completed, not how they were performed on a particular day.
- If well-known procedures were used, account for the procedure by name, possibly with a reference, and that's all.

Approach:

It is embarrassing to use vigorous voice when documenting methods without using first person, which would focus the reviewer's interest on the researcher rather than the job. As a result, when writing up the methods, most authors use third person passive voice.

Use standard style in this and every other part of the paper—avoid familiar lists, and use full sentences.

What to keep away from:

- Resources and methods are not a set of information.
- Skip all descriptive information and surroundings—save it for the argument.
- Leave out information that is immaterial to a third party.

Results:

The principle of a results segment is to present and demonstrate your conclusion. Create this part as entirely objective details of the outcome, and save all understanding for the discussion.

The page length of this segment is set by the sum and types of data to be reported. Use statistics and tables, if suitable, to present consequences most efficiently.

You must clearly differentiate material which would usually be incorporated in a study editorial from any unprocessed data or additional appendix matter that would not be available. In fact, such matters should not be submitted at all except if requested by the instructor.

Content:

- Sum up your conclusions in text and demonstrate them, if suitable, with figures and tables.
- In the manuscript, explain each of your consequences, and point the reader to remarks that are most appropriate.
- Present a background, such as by describing the question that was addressed by creation of an exacting study.
- Explain results of control experiments and give remarks that are not accessible in a prescribed figure or table, if appropriate.
- Examine your data, then prepare the analyzed (transformed) data in the form of a figure (graph), table, or manuscript.

What to stay away from:

- Do not discuss or infer your outcome, report surrounding information, or try to explain anything.
- Do not include raw data or intermediate calculations in a research manuscript.
- Do not present similar data more than once.
- A manuscript should complement any figures or tables, not duplicate information.
- Never confuse figures with tables—there is a difference.

Approach:

As always, use past tense when you submit your results, and put the whole thing in a reasonable order.

Put figures and tables, appropriately numbered, in order at the end of the report.

If you desire, you may place your figures and tables properly within the text of your results section.

Figures and tables:

If you put figures and tables at the end of some details, make certain that they are visibly distinguished from any attached appendix materials, such as raw facts. Whatever the position, each table must be titled, numbered one after the other, and include a heading. All figures and tables must be divided from the text.

Discussion:

The discussion is expected to be the trickiest segment to write. A lot of papers submitted to the journal are discarded based on problems with the discussion. There is no rule for how long an argument should be.

Position your understanding of the outcome visibly to lead the reviewer through your conclusions, and then finish the paper with a summing up of the implications of the study. The purpose here is to offer an understanding of your results and support all of your conclusions, using facts from your research and generally accepted information, if suitable. The implication of results should be fully described.

Infer your data in the conversation in suitable depth. This means that when you clarify an observable fact, you must explain mechanisms that may account for the observation. If your results vary from your prospect, make clear why that may have happened. If your results agree, then explain the theory that the proof supported. It is never suitable to just state that the data approved the prospect, and let it drop at that. Make a decision as to whether each premise is supported or discarded or if you cannot make a conclusion with assurance. Do not just dismiss a study or part of a study as "uncertain."

Research papers are not acknowledged if the work is imperfect. Draw what conclusions you can based upon the results that you have, and take care of the study as a finished work.

- You may propose future guidelines, such as how an experiment might be personalized to accomplish a new idea.
- Give details of all of your remarks as much as possible, focusing on mechanisms.
- Make a decision as to whether the tentative design sufficiently addressed the theory and whether or not it was correctly restricted. Try to present substitute explanations if they are sensible alternatives.
- One piece of research will not counter an overall question, so maintain the large picture in mind. Where do you go next? The best studies unlock new avenues of study. What questions remain?
- Recommendations for detailed papers will offer supplementary suggestions.

Approach:

When you refer to information, differentiate data generated by your own studies from other available information. Present work done by specific persons (including you) in past tense.

Describe generally acknowledged facts and main beliefs in present tense.

The Administration Rules

Administration Rules to Be Strictly Followed before Submitting Your Research Paper to Global Journals Inc.

Please read the following rules and regulations carefully before submitting your research paper to Global Journals Inc. to avoid rejection.

Segment draft and final research paper: You have to strictly follow the template of a research paper, failing which your paper may get rejected. You are expected to write each part of the paper wholly on your own. The peer reviewers need to identify your own perspective of the concepts in your own terms. Please do not extract straight from any other source, and do not rephrase someone else's analysis. Do not allow anyone else to proofread your manuscript.

Written material: You may discuss this with your guides and key sources. Do not copy anyone else's paper, even if this is only imitation, otherwise it will be rejected on the grounds of plagiarism, which is illegal. Various methods to avoid plagiarism are strictly applied by us to every paper, and, if found guilty, you may be blacklisted, which could affect your career adversely. To guard yourself and others from possible illegal use, please do not permit anyone to use or even read your paper and file.

Criterion for Grading a Research Paper (Compilation) by Global Journals Inc. (US)

Please note that following table is only a Grading of "Paper Compilation" and not on "Performed/Stated Research" whose grading solely depends on Individual Assigned Peer Reviewer and Editorial Board Member. These can be available only on request and after decision of Paper. This report will be the property of Global Journals Inc. (US).

Topics	Grades		
	A-B	C-D	E-F
Abstract	Clear and concise with appropriate content, Correct format. 200 words or below	Unclear summary and no specific data, Incorrect form Above 200 words	No specific data with ambiguous information Above 250 words
Introduction	Containing all background details with clear goal and appropriate details, flow specification, no grammar and spelling mistake, well organized sentence and paragraph, reference cited	Unclear and confusing data, appropriate format, grammar and spelling errors with unorganized matter	Out of place depth and content, hazy format
Methods and Procedures	Clear and to the point with well arranged paragraph, precision and accuracy of facts and figures, well organized subheads	Difficult to comprehend with embarrassed text, too much explanation but completed	Incorrect and unorganized structure with hazy meaning
Result	Well organized, Clear and specific, Correct units with precision, correct data, well structuring of paragraph, no grammar and spelling mistake	Complete and embarrassed text, difficult to comprehend	Irregular format with wrong facts and figures
Discussion	Well organized, meaningful specification, sound conclusion, logical and concise explanation, highly structured paragraph reference cited	Wordy, unclear conclusion, spurious	Conclusion is not cited, unorganized, difficult to comprehend
References	Complete and correct format, well organized	Beside the point, Incomplete	Wrong format and structuring

INDEX

save our planet

Global Journal of Computer Science and Technology

Visit us on the Web at www.GlobalJournals.org | www.ComputerResearch.org
or email us at helpdesk@globaljournals.org

ISSN 9754350