Preventing Man-in-The-Middle (MiTM) Attack of GSM Calls

B. I. Bakare and S. M. Ekolama

***Abstract* — Preventing man-in-the-middle (MiTM) attack using Artificial Neural Network refers to an in depth analysis of how calls are made vis-a-viz the structure of the inter-related operations that binds the respective subsystems within the GSM Architecture during calls. Calls in the GSM network is a request from a Mobile Station (MS). This request has faced severe attacks due to the network's access to Internet presence that has made its way into cellular telephony, creating a vulnerable and susceptible network attack such as Man-in-the-middle. This paper proffer solution to Man-in-the-middle attack during GSM calls by using Artificial Neural Network which can be embedded into the Protocol Stack to detect network intrusion and prevent Man-in-the-middle attack to obtain hitch-free local and international calls.**

***Key words* — Artificial Neural Network; Cellular Network; Communication; Gateway; Network intrusion.**

I. Introduction

Telephony involves deployment of technology for the purpose of telecommunication services such as transmission of voice, fax, or data, between remote parties. Telephony started from analog system to the present digital mobile network called the Global System for Mobile communication (GSM), which originated in Europe and spread to other parts of the world. According to Chan [1], telephony started as an analog AM radio phones called Walkie-Talkies to serve the military during World War II, which grew from analog system to digital system called GSM [2] and progressed from first Generation (1G) to the present fifth Generation (5G) network with target to provide data alongside voice services, SMS, and mms [3].

The thought of the primary cellular network was brainstormed in 1947. It was aimed at supporting the military as a way of providing troops with means of communications. From 1947 till around 1979 a few diverse types of broadcasting innovation surfaced. The United States came up with the AMPS (Advanced Mobile Phone Service) network, while European nations were creating their network of communication. In any case, when Europeans observed the drawbacks of each European nation working on their mobile network, it avoided cell phone utilize from nation to nation inside Europe. With the emerging European Union and fast-growing travel volume between nations in Europe, this was seen as big issue. Amending the situation, the Conference of European Posts and Telegraphs (CEPT setup a research team to investigate the mobile phone system in Europe. This group was known as Group Spécial Mobile (GSM). In 1989 work done by the GSM group was transferred to the European Telecommunication Standards Institute (ETSI). The title GSM was transposed to target the benefit the research was aimed to achieve. The acronym GSM had been changed from Group Spécial Mobile to Global System for Mobile Communications [4]. The term (GSM) has now included computer hardware, software, and computer network systems that toke over functions previously performed by telephone equipment which made possible Internet telephony, or VoIP, as result, the presence of Internet in telecommunications has raised security concerns, which this paper seeks to address

II. How GSM Functions

Global System for Mobile (GSM) Communications has brought colossal development within the Media transmission industry since it is conceivable for GSM clients to perform different administrations utilizing their communications gadget such as internet banking, videos streaming, high-speed internet activities etc. GSM has become a critical tool for financial and social resources, a basic instrument for transmitting or trading data for everyone. The persistent development and annually increment in GSM phones and other remote communication hardware in Nigeria and other parts of the world are great; it has brought the world into a global village [5].

Mitel, (n.d.) reported that GSM functions through a "variation of time division multiple access (TDMA), which is the foremost broadly utilized of the three digital wireless telephony technologies TDMA, GSM and code-division multiple access (CDMA)". The basic operation of GSM is its digitization and compression of data, which is then send down a channel with two other user data streams, each with its own time slot on the 900 MHz or 1,800 MHz frequency bands. GSM is part of the evolution of wireless mobile telecommunications, along with other wireless mobile telecommunications technologies such as High-Speed Circuit-Switched Data (HSCSD), General Packet Radio Service (GPRS), Enhanced Data GSM Environment (EDGE), and Universal Mobile Telecommunications Service (UMTS) (Rouse, n.d.).

III. GSM Architecture

The GSM Architecture is made up of three key subsystems: BSS (Base Station Subsystem), NSS (Network and Switching Subsystem), and OSS (Operation and Support Subsystem), as

Submitted on June 11, 2021.
Published on August 15, 2021.
B. I. Bakare, Department of Electrical Engineering, Rivers State University, Port Harcourt, Nigeria.
(e-mail: bakare.bodunrin@ust.edu.ng)
S. M. Ekolama, Department of Electrical Engineering, Rivers State University, Port Harcourt, Nigeria.
(e-mail: solomon.ekolama@ust.edu.ng)

indicated in Fig. 1, each of these systems has its own set of components:

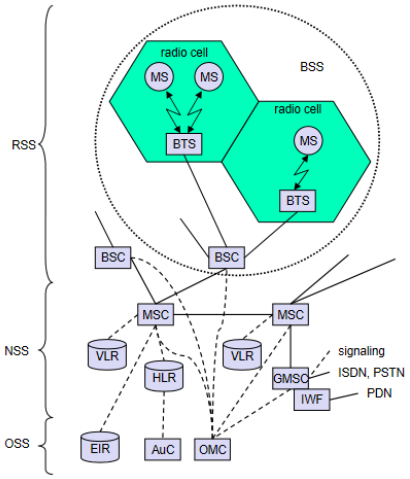

Fig. 1. GSM Architecture [8].

A. *Base Station Subsystem (BSS)*

Base Transceiver Station (BTS) and Base Station Controller make up the Base Station Subsystem (BSS) (BSC); these two components are used to "communicate over the designated Abis interface, allowing operations between components supplied by different providers" [9].

1. With clusters of small BTSs being deployed in major urban areas, the Base Transceiver Station (BTS) stores the radio transmitter, receivers, and their accompanying antennas to create a cell and manage the radio communication protocols with the Mobile Station (MS) through an interface called Um interface.

A BTS is typically positioned in the cell's center, with its transmitting power determined by the cell's size; additionally, each BTS contains between one and sixteen transceivers, depending on the density of users in the cell; and, finally, each BTS functions as a single cell [9]. Encoding, encrypting, multiplexing, modulating, and feeding RF signals to the antenna; Transcoding and rate adaptation; Time and frequency synchronization; Voice through full- or half-rate services; Decoding, decrypting, and equalizing received signals; Random access detection; Timing advances; and Uplink channel measurements are some of the functions of the BTS.

2. The Base Station Controller (BSC) is in charge of managing a group of BTSs' radio resources, including radio channel establishment, frequency hopping, and handovers. It connects the Mobile Station (MS) to the Mobile Switching Center (MSC). The BSC assigns and releases frequencies and time slots for the MS, transforming the 13kbps speech channel through the radio link to the standard 64 Kbps PSDN or Integrated Services Digital Network channel (ISDN). This approach is used to manage inter-cell handover and power transmission for the BSS and MS in its area.

B. *Network & Switching Subsystem (NSS)*

Call processing and subscriber-related operations are handled by NSS. It is essentially a data network that serves as the central control and interface for the entire mobile network. The Mobile Services Switching Center (MSC), the Home Location Register (HLR), the Visitor Location Register (VLR), the Authentication Center (AC), and the Equipment Identity Register (EIR) are all part of it (EIR) [10].

1. The Mobile Services Switching Centre (MSC) handles the system's telephony switching functions by acting as a switching node within a PSTN or ISDN, as well as other functions that support mobile users' needs such as registration, authentication, call location, inter-MSC handovers, and call routing to a mobile subscriber. It also handles calls to and from other telephone and data systems, as well as toll ticketing, network interfacing, and common channel signaling, among other things.

2. The Home Location Register (HLR) is a database that stores and manages information about subscriptions. It holds each subscriber's administrative information, including their last known location, and allows the MS to route calls to the appropriate base station. Although it may be distributed over several sub-centres for operational reasons, each network has only one HLR; consequently, when a person subscribes to a network, he or she is registered in that operator's HLR.

3. The Visitor Location Register (VLR) is a database that the MSC uses to give temporary information on subscribers on demand in order to service visiting subscribers. Although the VLR is usually implemented as part of the MSC, it can also be constructed as a separate entity. When a mobile station roams into a new MSC area, the VLR attached to that MSC will seek data from the HLR about the mobile station, and when the mobile station makes subsequent calls, the VLR will supply the relevant information without interrogating the HLR each time.

4. The Equipment Identity Register (EIR) is a database system that stores information on the mobile equipment's International Mobile Equipment Identity (IMEI) number (installed in the equipment and is checked by the network during registration). The EIR uses this data to determine if a piece of mobile equipment should be allowed into the network, blocked, or monitored in case of a problem.

5. The Authentication Centre (AuC) is a database that provides authentication and encryption parameters that verify the user's identity and ensure the confidentiality of each call using a secret key contained in the user's SIM card; "the AUC protects network operators from different types of fraud" by using this detail.

6. The Gateway Mobile Switching Centre (GMSC) is where a call is routed without knowing the MS's location outside the network upon termination, as well as where calls to subscribers outside the network are routed. Based on the MSISDN-Mobile Station ISDN number, the GMSC is responsible for obtaining the MSRN-Mobile Station Roaming Number from the HLR and routing the call to the appropriate visiting MSC.

Short Message Service (SMS) or Multimedia Messaging Service (MMS) Gateway (SMS-G) allows a Server (computer) to send and receive text messages between local and/or international telecommunications networks. The gateway controls two Mobile Switching Centres: one for sending short messages to Mobile Equipment and another for receiving short messages from a mobile on that network.

C. *Operation and Support Subsystem (OSS)*

The Operation and Support Subsystem (OSS), also known as the operations and maintenance center (OMC), is a control

and monitoring system for the overall GSM network as well as the BSS traffic load. It is connected to all switching system equipment as well as the BSC [11], [12].

The OSS gives network operators access to the system for monitoring and control, allowing them to provide customers with cost-effective support for centralized, regional, local, and operational service, as well as GSM network maintenance.

Administration and commercial operation (subscription, and terminals, charging, and statistics), Security Management, Network configuration, Operation, and Performance Management, and Maintenance Tasks are some of the other roles of the OSS [7].

IV. Cellular Network Structure

According to Albert & Indra [13], "cellular telephone networks extend the basic telephone service to mobile users with portable telephones" (p. 239), through the telephone number that specifies the particular Mobile Station as shown in figure 7.

From the base transceiver station (BTS) with its antenna back through a base station controller (BSC) and a mobile switching centre (MSC) to the location registers (HLR and VLR) and the links to the public switched telephone network (PSTN), the overall cellular network contains a number of different elements.[14].

In cellular telephony, Albert, and Indra [13] proposed that a city, for example, can be partitioned into a number of geographical sections called cells. Large cells are designated in rural areas, whereas clusters of smaller cells are designated in urban areas, based on the density of subscribers.

A Base Station is located at the cell's center to connect the Base Station, which in turn connects to a Base Station Controller, which serves as a hub for routing calls to the appropriate base station and making decisions about which base station is most suited for a given call. The link between the BTS and the BSC is normally a microwave link, and antenna support for the BSC is frequently co-located with the BTS. As a result, widespread decisions about call and interface routing to the basic PSTN, as well as the HLR and VLR, are made, as shown in the GSM Protocol Stack.

V. GSM Protocol Stack

The GSM architecture is layered in such a way as to allow communication within and between different Networks. To accomplish this, the architecture is divided into three layers [13], each of which communicates with the others using standard protocols. As a result, the lower layers of the network ensure that the upper-layer protocols' services are provided, and each layer sends appropriate notifications to ensure that transmitted data is properly formatted, transmitted, and received.

The GSM protocol stack is the network interface that allows for call setup. Each Mobile Station receives an HLR, which contains the user's position and subscription services, as well as a VLR, which is a distinct register used to track a user's location. When users leave the region covered by the HLR, the MS notifies the VLR, who then searches for the user. The VLR, in turn, notifies the HLR of the MS's new location using the control network. Mobile termination (MT) calls can be routed to the user using the information included in the user's HLR [13].

VI. Call Flow in GSM Network

The process through which a call is routed in a GSM network to a mobile device is known as call flow, which can take place either in a CDMA network or LTE network [13], as shown in Fig. 2 below.

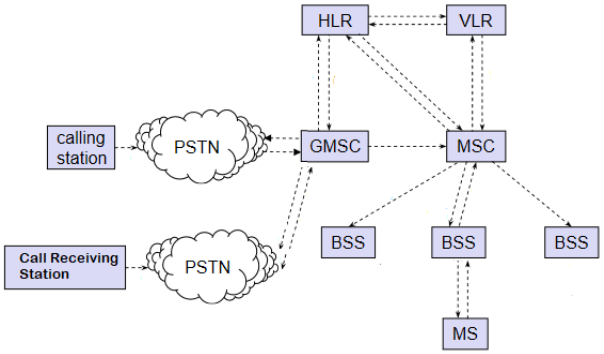

Fig. 2. GSM Call Flow [8].

A. Local Calls

Initiating a call in the GSM network starts from the mobile station sending a request in the reverse setup channel, with the requesting MS phone number, as well as the destination phone number, in addition to a serial number and possible password information which are transmitted to the MSC to validate the request which initiates the call setup. This call setup necessitates consulting the home location register, which is database containing information about subscribers whose home area is this one. The authentication center, which stores authentication information about subscribing to traditional telephone signaling, is used to validate the system, and the base station and mobile station are relocated to their allotted forward and reverse speech channels [13].

The user is authenticated after the base station receives this response, and the mobile switching center (MSC) sends an initial address message to the network via the GSMC, and the call is routed to the correct switching center, causing the network to generate an Address Complete Message (ACM) as soon as the correct switching center is located. When the MSC receives this communication, it notifies the base station, which notifies the caller's mobile phone, causing the earpiece to ring. The MSC notifies the caller's mobile device to transmit voice on the allotted traffic channel if the called party answers.

B. Handover in GSM Network-Local Calls

The signal strength is checked by the base station while the call progresses, according to Albert & Indra [13]. If the signal strength falls below a certain threshold, the MSC is notified, and the mobile station is told to transmit on the setup channel, while all nearby base stations are instructed to check the signal strength in the prescribed setup channel. As a result, the MSC uses this information to determine the best cell to which the call should be transferred; as a result, the current

base station and the mobile station are instructed to prepare for a handoff; once they are ready, the MSC releases its connection to the first base station and establishes a connection to the new base station, and the Mobile Station changes its channel to those selected.

C. International Call (Roaming)

Because of bilateral business arrangements between the home and visited cellular service providers, which then automatically provide roaming service, and a series of interactions required between the home network and the visited network using the telephone signaling system, communication between different mobile operator network regions is possible. When the roamer enters a new region, the setup channels are used to register the roamer. The roamer's information is used by the MSC in the new area to request authorization for the roamer's home location register. The visitor location registration keeps track of subscribers who come to visit. The roamer can then receive and make calls inside the new area after registering [13].

The location of a device in a GSM network is highly significant, as location updating is needed for roaming of the MS from one location region area to another; whenever this occurs, a mobility and handover function is required to transfer services between the locations [13]. The MS is always listening to radio network signals (to see whether it has been paged for an incoming message) and communicating its location to the radio network whenever it reaches a new region [14]. The procedure for handover is as follow:

- "The MS connects to the radio network and sends a location update request to the current BSS to communicate with the network.
  The BSS sends the request to the MSC, which discovers that the device was previously registered with another MSC/VLR.
- By providing the Temporary Mobile Subscriber Identity, the current MSC contacts the prior MSC to obtain information about the MS.
- The IMSI is associated with the TMSI in the previous MSC, therefore the IMSI parameter is supplied to the new MSC. The current location of the device is updated in the HLR as it reaches the MSC; with the IMSI number, the HLR can give information about the subscriber (services authorized, preferences, etc.) to the new MSC.
- The HLR information from the prior MSC/VLR is erased, and the new VLR location is updated.
- Authentication is accomplished using the SIM card and IMSI after the HLR has sent the modifications to the new MSC. Following authentication, the MSC begins ciphering and assigns a new temporary identity to the subscriber, which will be used to update their next location".

Handover between two separate MSCs might also be requested. When the BSC receives notification of a location change and determines that the new location is not in its service area, it sends the handover request to the MSC, who confirms that the subscriber has roamed to a different MSC. Because the MSC has access to the LACs of nearby MSCs, it may tell which network the subscriber has wandered in.

The old MSC makes a request to the target MSC, which instructs the relevant BSC to build a speech channel for the MS; the MS receives the handover request via the previously established channel; communication is transferred to the newly constructed channel of the second MSC. All inter-MSC handover processes that may occur during a call are the responsibility of the MSC that initially assigned the MSRN for establishing up the call, known as an anchor MSC.

VII. GSM Network Attacks

Cellular network with all its attendant benefits also has its challenges. The advent of the advanced networks that operates on packet switched which are connected to external networks like the Internet especially as 5G technology is gaining wider adoption makes the network vulnerable to different types of attacks including Man-in-the-Middle attack.

Man-in-the-Middle attack poses real threat to wireless network security and cellular Network in particular. It's when an attacker "intercepts communications between two parties in order to steal login credentials or personal information, spy on the victim, or hijack communications sessions" [12], [17] as shown in Fig. 3 below.

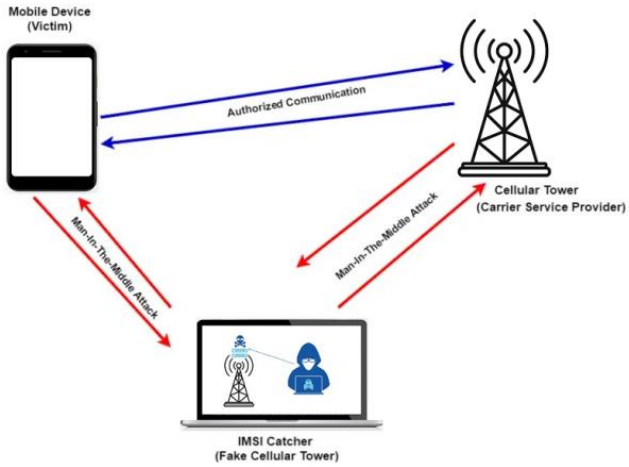

Fig. 3. Man-in-the-middle Attack.

VIII. Proposed Solutions to Man-in-the-middle (MITM) Attack

The key to avoiding MiTM assaults is to have a reliable intrusion detection system in place. An intrusion is defined as any attempt to undermine network security (for example, data confidentiality, integrity, and authentication). Intrusion detection (ID) techniques are used to improve the security of a system and make it more resistant to attacks. Intrusion detection systems (IDSs) are used to implement these strategies. In general, the fundamental objective of an intrusion detection system is to detect an intrusion and, if required or possible, to take steps to eradicate it. [18].

Artificial Neural Network Algorithm has been found to play the role of IDS, strengthen cellular network security and prevent intrusion that may lead to MiTM attacks.

A. Implementing Artificial Neural Network to prevent MiTM attack

As depicted in Fig. 4, a neural network is a set of algorithms designed to recognize the underlying relationships

in a set of data using simple elements or nodes known as neurons. “The Neural Network's function is mostly governed by the connections between the neurons. These neurons are linked together by links, each of which is regulated by weights, and the process of updating the weights is known as learning” [18].

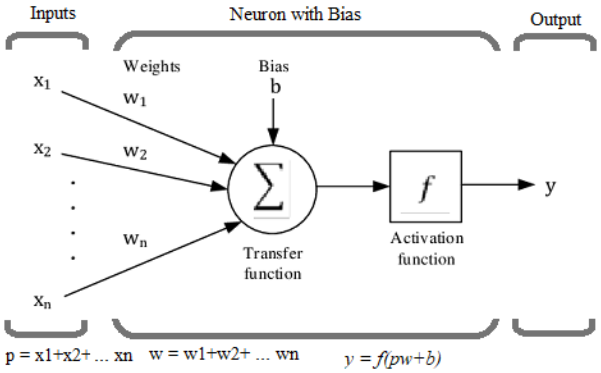

Fig. 4. Simple Neuron Model.

The neuron, n, is made up of inputs p, weights w, and a scalar bias b, as shown in figure 4, and serves as an input (i.e., n=wp+b) to the transfer function. The transfer function is passed to an activation function f, which produces the output, y of the neuron. Consequently, the artificial neuron equation becomes:

$$y = f(n)$$

where “f” is a transfer function that takes “n” argument and produces “y” output, as shown in the equation. The Neural Network's intended behaviour is produced by modifying its weight or bias settings as a training method to reach a desired result.

To augment n, which becomes the input to the neuron transfer function, the input p to the neuron can be increased to R-elements input and each input is multiplied by weight. The increased n will look like this:

$$n = (W_{1,1}P_1 + W_{1,2}P_2 + W_{1,3}P_3 + \cdots W_{1,R}P_R) + b$$

which becomes the new input, n to the neuron transfer function as shown in Fig. 5.

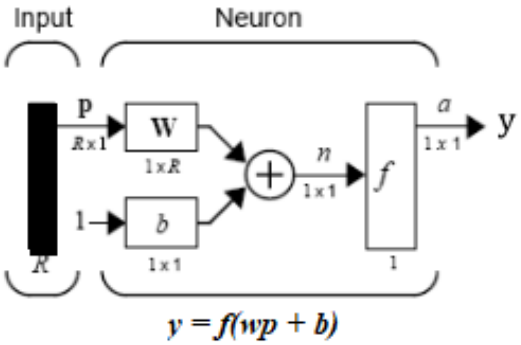

Fig. 5. Single layer neuron with augmented n [18].

The single layered neuron of Fig. 5 can be enhanced by adding multiple layers to form a multilayered neuron as shown in Fig. 6.

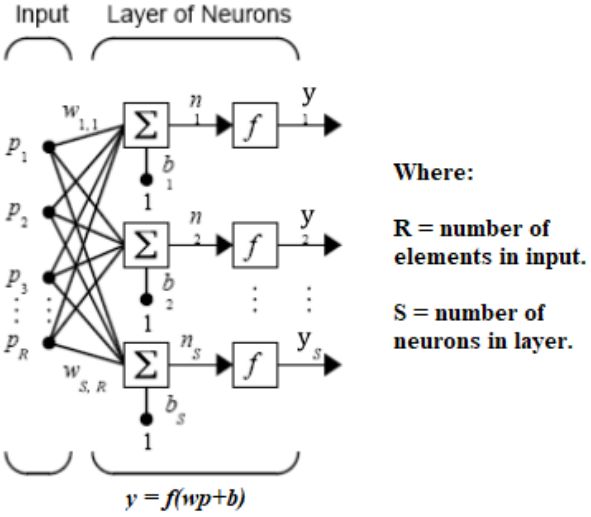

Fig. 6. Multilayer Neuron [18].

The Fig. 6 Neuron can be bundled into a feed-forward system to enhance the Artificial Neural Network architecture for improved network security as shown in Fig. 7.

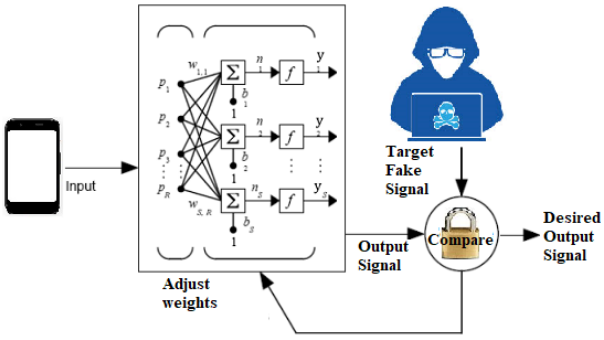

Fig. 7. Multilayered Neural Network Architecture.

Fig. 7 shows a Multilayer feed-forward network that belongs to the “Networks for Classification and Prediction” network category. [18], which can be used as intrusion detection technique to predict the behaviour of an intruder a network system.

Consequently, the Multilayer Neural Network, can be embedded in the GSM Protocol Stack and act as a key to detect intrusion and select the desired signal to output to the channel requesting call setup, this way, it is able to prevent MiTM attack as shown in Fig. 8.

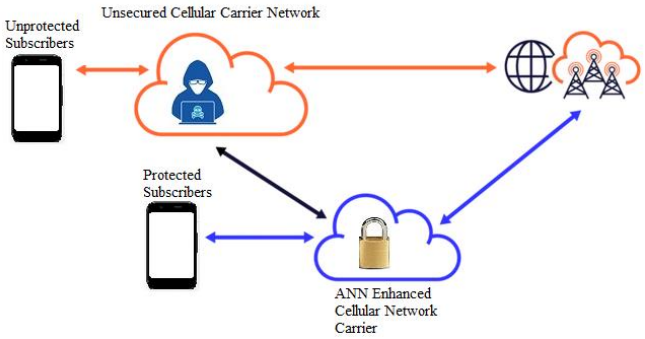

Fig. 8. Secured cellular carrier network.

IX. CONCLUSION

The GSM network has long changed the way we interact and socialize. Thanks to mobile phones, calls can now be made locally and internationally, especially with the advent of the advanced networks such as 5G that operates through circuit and pack-switched networks that have made communication in its entire entirety seamless. An X-Ray of the GSM network revealed that irrespective of the successes brought by the GSM network, it also has its flaws that possess threats, such as Man-in-the-Middle attacks that raise high security concern. Consequently, we developed a multilayer neural network architecture, which can be embedded into the protocol stack of the GSM network architecture to solve the problems of network intrusion, which will help to overcome all security challenges and pave the way for full benefits cellular network communication.

REFERENCES

[1] Chan, A. S. (2018). A brief history of 1G mobile communication technology. https://blog.xoxzo.com/en/2018/07/24/history-of-1g/.
[2] Temple, S. (2010). Inside the Mobile Revolution: a Political History of GSM. http://www.gsmhistory.com/wp-content/uploads/2013/01/Inside-a-Mobile-Revolution-Temple-20101.pdf.
[3] Munir, M. W. (2005). Different Generations of Cellular Networks System. https://www.researchgate.net/publication/276319644_Different_Generations_of_Cellular_Networks_System/references.
[4] B.I.Bakare, I.A Ekanem and I.O. Allen (June, 2017). Appraisal of Global System for Mobile Communication in Nigeria, *American Journal of Engineering Research*. [Online]. 6(6), pp. 97-102. Available: http://ajer.org/papers/v6(06)/N060697102.pdf.
[5] B.I. Bakare, Sunny Orike and D.I. Oko (January, 2020). Evaluation and Analsis of the deployment of Green Communication Technology in GSM, *European Journal of Electrical and Computer Science*. [Online]. 4(1), pp. 1-9
[6] Mitel. (n.d.). What is Telephony? https://www.mitel.com/features-benefits/telephony.
[7] Rouse, M. (n.d.). GSM (Global System for Mobile communication). https://searchmobilecomputing.techtarget.com/definition/GSM.
[8] Leitao, M. J. (n.d.). Mobile Communication Systems: GSMGlobal System for Mobile Communication. https://web.fe.up.pt/~mleitao/CMOV/Teoricas/CMOV_GSM.pdf.
[9] Tutorialspoint.com (n.d.). GSM - Architecture. Retrieved from https://www.tutorialspoint.com/gsm/gsm_architecture.htm.
[10] Tipper, D. (n.d.). Global System for Mobile (GSM) (GSM). http://www.pitt.edu/~dtipper/2700/2700_Slides8_2.pdf.
[11] Shaikk, S., Chaudhari, N., & Patil, P. (2016). Modeling of Operation Support System (OSS) for Business Management and Automation. International Journal of Research in Management, ISSN 2249-5908 Available online on http://www.rspublication.com/ijrm/ijrm_index.htm Issue 6, Vol. 5 (September 2016).
[12] Toorani, M. and Beheshti, A.A. (2008). Solutions to the GSM Security Weaknesses. Proceedings of the 2nd International Conference on Next Generation Mobile Applications, Services, and Technologies (NGMAST'08), pp.576-581, University of Glamorgan, Cardiff, UK, Sep. 2008 [DOI 10.1109/NGMAST.2008.88].
[13] Albert, L. and Indra, W. (2000). Communication Networks. McGraw-Hill Higher Education.
[14] Electronicsnotes. (n.d.). GSM Network Architecture. https://www.electronics-notes.com/articles/connectivity/2g-gsm/network-architecture.php.
[15] Zhao, W. (1997). Handover Techniques and Network Integration between GSM and Satellite Mobile Communication Systems. https://core.ac.uk/download/pdf/102784.pdf.
[16] Yatebts.com. (2019). GSM Functionalities. Retrieved from https://yatebts.com/documentation/concepts/gsm-functionalities/.
[17] Gardezi, A. I. (n.d.). Security In Wireless Cellular Networks. Retrieved from https://www.cse.wustl.edu/~jain/cse574-06/ftp/cellular_security/index.html.
[18] Alfantookh, A. A. (2006). DoS Attacks Intelligent Detection using Neural Networks. J. King Saud Univ., Vol. 18, Comp. & Info. Sci., pp. 27-45 (A.H. 1426/2006).

B. I. Bakare holds a Bachelor of Engineering (B.Eng.) Degree in Electrical Engineering; 2/1 from Ondo State University, Ado Ekiti, (Now University of Ado Ekiti, Ekiti State), Master of Engineering (M.Eng.) Degree in Electrical/Electronic Engineering from University of Port Harcourt, Nigeria and he is currently a PhD (Communication Engineering) Researcher of Nnamdi Azikiwe University (Unizik), Awka, Anambra State. He holds a Category One Wiring License. He is a COREN registered Engineer, a Corporate Member of Nigeria Society of Engineers (NSE), a member of International Association of Engineers (I A ENG) and an active member of Nigeria Institute of Electrical and Electronics Engineers (NIEEE). He is presently a lecturer in the Department of Electrical Engineering, Rivers State University, Port Harcourt., Nigeria.

S.M. Ekolama holds a Bachelor of Technology in Engineering (B. Tech.) Degree in Agricultural Engineering from Rivers State University of Science and Technology, (Now Rivers State University, Port Harcourt), Post Graduate Diploma (PGD) in Electrical Engineering, from Rivers State University of Science and Technology, (Now Rivers State University, Port Harcourt). He is currently pursuing Postgraduate studies (M. Tech) in Communication Engineering at River State University He is a COREN registered Engineer, a Corporate Member of Nigeria Society of Engineers (NSE), a member of International Association of Engineers (I A ENG) and an active member of Nigeria Institute of Electrical and Electronics Engineers (NIEEE). He is presently at the Department of Agricultural and Environmental Engineering, Niger Delta University, Wilberforce Island, Bayelsa St State, Nigeria.