EAI Endorsed Transactions
on ______________________________ Editorial ICST.ORG

Africa: cyber-security and its mutual impacts with computerisation, miniaturisation and location-based authentication

M.I. Adeka[1,*], K.O.O. Anoh[1], M. Ngala[1], S.J. Shepherd[1], E. Ibrahim[2], I.T.E. Elfergani[3], A.S. Hussaini[3], J. Rodriguez and R.A. Abd-Alhameed[1]

[1]Mobile and Satellite Communications Centre, University of Bradford, UK
[2]College of Electronic Technology Bani Walid – Libya
[3]Instituto de Telecomunicacoes – Aveiro, Portugal

Abstract

The state of insecurity occasioned by fraudulent practices in Africa has been of concern economically, both at home and abroad. In this paper, we propose ways to mitigate this problem, using Nigeria as a case study. Based on surveys in West Africa, the paper examines the security situation in the continent and its mutual impacts with computerisation, miniaturisation and Location-Based Authentication (LBA). It was discovered that computerisation and miniaturisation had negative effects on cyber-security, as these were being exploited by fraudsters, using *advance fee fraud*; called *419*. As a countermeasure, the paper examines the possibility of using LBA and digitisation of the GSM Mobile country codes down to city/area codes along with GSM/GPS authentications. These could also be combined with the use of a web-based Secret Sharing Scheme for services with very high security demands. The challenges of roaming were also examined and considered to be of negligible impact.

Keywords: cyber space, computerisation, miniaturisation, authentication, advance fee fraud (419), digitisation and tele-density.

1. Introduction

The degree of cyber-related insecurity occasioned by fraudulent practices in Africa has been an issue of great concern economically, especially as it relates to foreign direct investments and dealings with other international partners. Apart from the economic costs to the nations, corporate organisations and individuals, it has also dented the image of some of the countries in various international fora. This motivation of this paper is an effort to find ways of using technology to mitigate the negative effects of this state of insecurity. Although the study samples have been drawn from the West African community, specifically, using Nigeria as a case study, the results are applicable to all countries with similar situations.

Based on surveys involving two field trips to Nigeria and the knowledge acquired via the implementation of CDRSAS-PT (Cloud Data Repository Secure Access Service - Prototype; a recently-completed PhD Research Project [1]), among other resources, this paper begins by examining the general security situation in the regional environment, with a focus on cyber-security, especially as it relates to the use of Global System for Mobile Communications (GSM). We then give some basic clarifications of some relevant concepts, including cyber space, computerisation, miniaturisation, Location Based Authentication (LBA), advance fee fraud (419), digitisation and tele-density, as they affect the sub-Saharan nations, with Nigeria as the hub of activities. In Section 3, both the forward and backward effects of these technological developments are then assessed *vis-a-vis* the national security posture with a focus on the security of cyber space. In Section 4, the discussions on identifiable measures aimed at mitigating possible security threats in the system are presented. These include the possibility of using LBA and further digitisation of the GSM Mobile country codes down to City/Area codes along with GSM Mobile/Global Positioning System (GPS) authentications. Where necessary, these could be combined with the use of a web-based Secret Sharing Scheme for services with very high security demands. Possible challenges to the suggested mitigating measures would also be considered in Section 5 with the conclusion following in Section 6.

[*] M.I. Adeka, miadeka@student.bradford.ac.uk

2. Basic conceptual clarifications

The term *cyberspace* does not have a standard and objective definition [2]. Generally, it is used to describe the virtual world of computers. In other words, while the term *'cyber'* denotes the computer and anything that relates to it, *cyberspace* refers to the notional environment in which communications over computer networks occur [3]. It is "the domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange data via networked systems and associated physical infrastructure" [1]. On the other hand, *computerisation* is to cause certain operations or processes to be performed by a computer, particularly, as a replacement for human labour. *Digitisation* is the process of converting real-world analogue quantities (texts, images, audio, video, etc.) into a digital format [4]. In this format, information is organised into discrete small units of data (bits) which are grouped into bytes. This is the binary data that computers and several devices with computing capacity can process. Thus, digitisation involves a process that results in the breaking down of a given whole into its smaller parts.

Miniaturisation is the continuous reduction in the sizes of manufactured items, regardless of whether they are mechanical, optical or electronic products and devices; e.g., mobile phones, computers, vehicle engine downsizing, etc. [5]. This trend is made possible by the emergence of *micro* and *nano* technologies. *Authentication* is the process of establishing the true identity of a user or an entity [6]. Thus, LBA is a form of authentication where the identification factor is related to the physical location of the user/entity. Tele-density used to be computed as the number of fixed telephone lines per hundred inhabitants. With the advent of GSM, where mobile cellular subscribers outnumber the fixed line connections in some countries, the term Mobi-density is preferred in such countries; i.e., mobile cellular subscribers per hundred inhabitants. Since the two terms may lead to mutual disadvantages for countries with well-established fixed lines and those whose GSM network is still at the initial stage of development. ITU has proposed the use of Effective Tele-density; defined as either fixed line connections or mobile subscribers per hundred inhabitants – whichever of the two is higher [7], [8].

Advance fee fraud (alias 419), which is also known as the *Nigerian Scam*, has grown into an epidemic [9]. The term *'419'* was coined from Section 419 of the Nigerian Criminal Code (part of Chapter 38: Obtaining Property by False Pretences; Cheating) [10]. Basically, 419 is a form of confidence trick which the confidence *artists* use to defraud unassuming innocent business partners, both locally and abroad. An example of a 419-transaction is illustrated in Figure 1, where *Caller 2* (Location B; Lagos) gives his fake location as *Kano* (Location E) in his mobile phone conversation with *Caller 1* (Location A; Ibadan); while he is actually speaking from *Lagos.* Please note that *Caller 2* could have given his fake location as Locations C (*Kumasi* in Ghana) or D (*Niamey* in Niger), claiming to have roamed his mobile service.

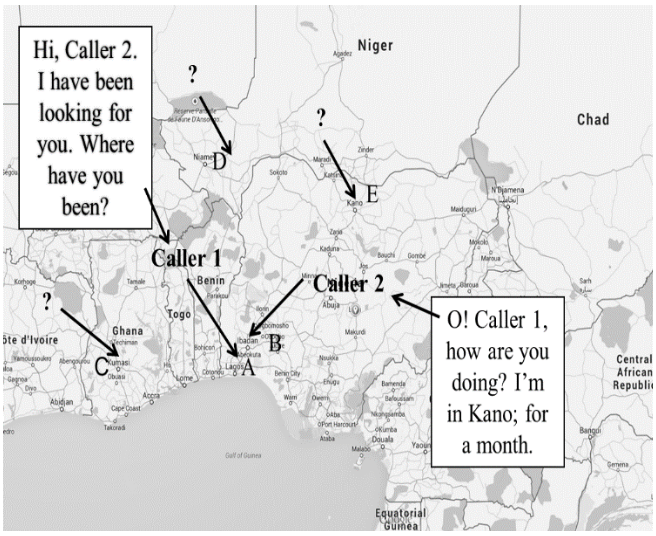

Hi, Caller 2. I have been looking for you. Where have you been?
Caller 1
Caller 2
O! Caller 1, how are you doing? I'm in Kano; for a month.
?
?
?
A
B
C
D
E
Niger
Chad
Benin
Togo
Ghana
ôte d'Ivoire
Central African Republi
Equatorial Guinea
Gulf of Guinea

Figure 1. A 419 mobile phone conversation: giving a fake caller's location

3. The state of cyber insecurity in Africa, using Nigeria as a case study

Every society has its bad eggs; research estimates show that about 4% of Nigerians engage in cybercrimes [11]. It is clear from the magnitude of this percentage that, the 419 fraud is a major concern, not only for African Governments and their citizens, but the entire global community [10].

Cybercrime refers to any unlawful act perpetrated using the computer, electronics and ancillary devices as tools within the cyberspace [12]. It involves disruption of network traffic along with virtually an endless list of major and sundry crimes including terrorism and outright warfare [3]. It targets individuals, individual properties, corporate organisations, governments, the entire nation and the global community at large [3, 12]. Discussions with and statistics from the Economic and Financial Crimes Commission (EFCC), Abuja, and the Special Fraud Unit (SFU) of the Nigeria Police, Lagos, Nigeria, indicate that cybercrimes that are prevalent in Nigeria include [13, 14]: *fishing* and *spoofing* activities targeting bank customers; skimming of standard issue magnetic-stripe ATM (Automated Teller Machine) cards; cloning and/or defacing of government and business websites; spamming activities involving 419 solicitations (for lottery, inheritance, charity, romance, crude oil, fund transfer, employment, contracts, etc.); fraudulent online purchases from e-commerce sites made with fake foreign financial instruments and stolen credit card information; online investment scams targeting local victims; deployment of malicious programmes – mostly off-the-shelf spyware, key stroke loggers, Trojans and extractors on target systems; targeting of emotionally vulnerable persons on free social networking sites; and the use of free email services (especially g-mail, yahoo-mail and hotmail) in cybercrime related communications.

Cybercrimes are very common in Nigeria but they could appear elsewhere. Statistics reveal that these crimes are mostly committed by males between the ages of 20–35, and mostly based in University towns [13]. Nigeria currently ranks first in Africa, and third in the world, after the US and UK, with 5.7% cybercrime perpetrators (down by 0.2% from 2006), as illustrated in Table 1 [12].

Table 1. Top Ten Countries by Count (Cybercrime Perpetrators)

Country	Percentage
1. United States	63.2%
2. United Kingdom	15.3%
3. Nigeria	5.7%
4. Canada	5.6%
5. Romania	1.5%
6. Italy	1.3%
7. Spain	0.9%
8. South Africa	0.9%
9. Russia	0.8%
10. Ghana	0.7%
Source: Internet Crime Report 2007	

Table 2. Cyber Fraudulent Crime Statistics in Nigeria (EFCC/NFIU) - 2012 – 2014

Year	Description	Quantity
2012	No of Cases Reported No of Suspects Arrested Financial Recoveries (Naira)	89 100 2.4 Billion
2013	No of Cases Reported No of Suspects Arrested Financial Recoveries (Naira)	99 188 8.4 Billion
2014*	No of Cases Reported No of Suspects Arrested Financial Recoveries (Naira)	93 - 630 Million
Source: Nigeria Police (SFU) and EFCC Crime Statistics **2014*** … For the First Quarter Only		

From Table 2, all the indices for the incidence of cybercrime in Nigeria are on the increase for the three years shown; some astronomically, bearing in mind that the indicators for 2014 are incomplete. Virtually all researchers agree that globalization occasioned by the revolution in Information and Communication Technology (ICT) has greatly contributed to the rise in cybercrimes globally. However, this does not explain why Nigeria should be far ahead of South Africa, for instance, with 5.7% against 0.9%, given that the Internet users in South Africa are more than 50% of their Nigerian counterparts: about 26.5% of Nigerians use the Internet, giving about 45million Internet users; South Africa has about 48.9% of its population on the net, yielding about 23.6 million users [15]. Many researchers agree that it is the Nigerian 419 Scam that has sharply differentiated her from South Africa, and this was enhanced by miniaturization of communication devices among other factors, especially the mobile phone which is very portable and more amenable to deception in respect of callers' geo-location information [10 - 13].

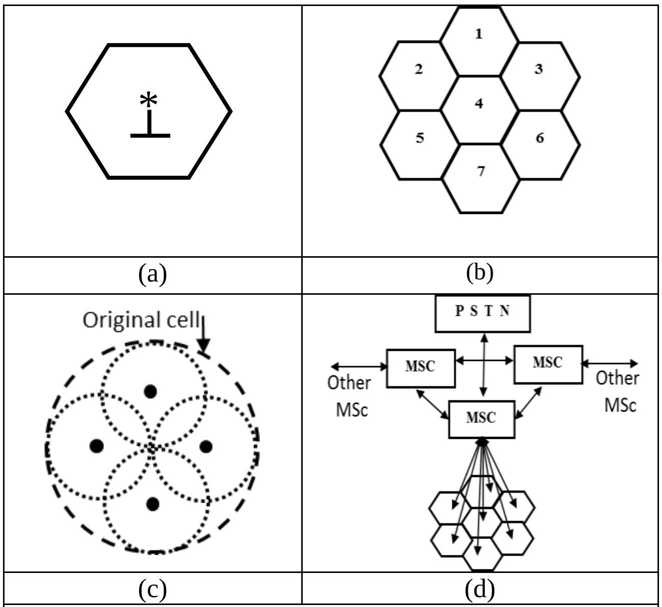
The implication of this finding can be fully appreciated only if it is realized that, the annual statistics for mobile phone subscribers in Nigeria indicates a leap from 266,46 to 135,253,599 between 2001 and 2012, respectively. The effective tele-density for the corresponding periods also witnessed a quantum leap from 0.73 to 80.85 respectively [16]. Nigerian Governments have been fighting fraudulent crimes for a long time without much result. This led to the establishment of various outfits, in addition to the Nigerian Criminal Code Act. Thus, it could be said that while globalization has enhanced the socio-economic life of the people, it has also come along with insecurity problems that have so far defied solutions.

4. Countering feigned-location fraud related crimes in Nigeria

It is noteworthy that most of the measures so far employed in Nigeria to counter the cyber and other fraud-related crimes are mostly based on legal instruments; in terms of enactments and enforcements. Since the most valuable tool for the 419 fraudsters is the mobile phone, it seems reasonable to approach the problem from a technological angle as one of the most promising ways forward. It is hereby proposed that location-based authentication be employed in two versions in Nigeria. While one version is to actually detect the exact physical location of the fraudster, the other is to deter him/her from committing the crime. For actual detection, there would be need to make all transceivers GPS-compliant, with inherent capabilities for location-based mutual authentication as advocated in [6]. This would be able to detect the locations of both static and mobile cyber criminals; please note that a mobile phone is being treated here as a computer – smart phones are computers with phone capabilities. The deterrence approach would be realised by a further digitisation of the country codes for the GSM cellular phone systems, as explained in the next section. This could be very effective against 419 fraudsters who use the mobile phone as their main tool. Where necessary, the two approaches could be combined with the use of a modified web-based secret sharing scheme for services with very high security demands.

4.1 Background to the deterrence approach

In the evolution of cellular phones, one major reason for dropping certain standards stemmed from security limitations and incompatibility of diverse standards. Researches were motivated to solve this challenge. Breakthroughs yielded the Long Term Evolution (LTE) today [17, 18]. Since then, subsequent cellular standards have become more mobile, secure and compatible with earlier standards across different national boundaries. Aside from these improvements, security challenges still abound such as location identification of a mobile user. Recently, the 3GPP working group proposed the inclusion of the Time Difference of Arrival (TDOA) algorithm [19] in the LTE-Advanced (LTE-A) Release 10 and beyond (which has been revised to inherit Rel-8/9 features) to identify the location of a mobile caller [20, 21]. In cellular phone networks, although the term Enhanced Observed Time Difference (E-OTD) is often used instead of TDOA, the principle is the same [6], except that the former involves the broadcast of cell-ID [21].



(a) (b) (c) (d)

Figure 2. Hierarchical Structure of Cellular Network: (a) Base Station (BS) for a Cell; (b) A 7-Cell Cluster; (c) Cell Splitting; and (d) Cellular Network Structure

In contrast to mobile phones, fixed telephones are more secure and mostly preferred in official involvements, since it is more accurately traceable. Its address can be easily found since the address (including the city codes) assigned to a user is known. This feature makes it more dependable to transact businesses using fixed telephones than mobile phones. This proposal considers mapping the security advantage of the fixed telephones on to the mobiles (with a variety of modifications) such that it can be more dependable in this respect. Of course, most business organizations would benefit should the mobile lines provide equivalent levels of security to fixed lines.

In the meantime, area codes are known to be common and are defined differently for different countries [22,23]; e.g., three digits for USA, Canada and Nigeria, two digits for Brazil and one digit for Australia and New Zeeland. We also have variable lengths for United Kingdom, Germany, Austria, etc. Sometimes, and in some countries also, these area codes are part of caller's mobile number. It is hoped that another variety can be exploited that would travel with the permanent caller mobile number. It is possible that this research may revolutionize area/city coding for mobile nodes and that the security breaches volunteered by the cellular telecommunication security orifice will be solved permanently, within the context of current technology.

This proposal does not suggest any change in the numbering plan or hardware of any telecommunication network operator, but integration into the software configuration of the radio routing elements of the network operator's systems – base station (Node-B, evolved-Node B or Home-eNB). It does not affect the traditional design of the mobile handsets nor would the handsets be reconfigured for the purpose.

4.2 Benefits to the Country

From experience, the duo of *location-based identification* and *mobility* has always been a confidence-inspiring pair of factors for criminals; the mobile communication technology is no exception. This is because prompt identification of the geographical position of the mobile phone users is still a technology challenge, which is consequent upon mobility and positioning. Most crimes in Africa are therefore aided and/or perpetrated using mobile phones. Such crimes include kidnapping, robbery, impersonation, terrorism and all shades of '419'. Sometimes, family members masquerade to defraud own family. Debtors pretend to abide in Abuja while in Lagos. The ban on the use of GSM/Thuraya services in Borno, Yobe and Adamawa States in the wake of the State of Emergency (SoE) declared in May 2013 (Nigeria), is a robust illustration of the argument being canvased in support of this proposal. Hence, this proposal means a solution for reducing the tendency to commit the crimes associated with the use of mobile phones to enhance confidence in the committing of such crimes in the country. It is instructive to note that the deterrence effect of the technological solution envisaged in the proposal, is even more than its enhancements in tracking down the criminals with a view to subjecting them to justice. This proposal would be an obituary for '*419 and Associates*,' not only in Africa, but the world at large.

4.3 The proposed technology

In the meantime, a mobile phone caller can be traced to the country of origin using the country calling code. It makes it very possible that fraudulent activities can thrive since the exact location of the mobile caller cannot be estimated by the ordinary users. In LTE-A Release 10 and beyond, mobile phones are proposed to incorporate the TDOA in determining the location of the mobile caller [20, 21]. This tracking functionality permits that only the network operators and/or the security agencies such as the police would be able to trace the origin of a mobile caller, depending on the TDOA parameters [19] extracted from the caller. It can be reasoned that this still makes the acquisition of the space-time information of a mobile caller vague, perilous, tedious, and expensive. The proximity of a caller's location characteristics to the parameters extracted from the TDOA algorithm cannot define the position of a caller closer than 10 meters. In addition, the time it takes to compute and then trace the origin of the caller can as well leverage fraud. The proposed initiative can be combined with the TDOA to improve the identification of a mobile user's geographical location faster. In fact, at least four cells are required to perform Observed Time Difference of Arrival (OTDOA) [19,24], and the disadvantages cannot be overstressed.

Just like the landlines wherein a caller location can be easily identified, a similar situation is being advocated for a mobile user. This could be achieved by a further digitisation of the GSM country code into city/area codes. Thus, the caller ID travels with the city/area codes as well, instead of country code alone. With proper public awareness education, it would become clear to all users that such phones could no longer be safely used in defrauding people by falsifying the city location of the caller. The exact city location can be extended to a mobile phone user to reduce and also discourage fraudulent activities among mobile phone users. The city/area codes will be incorporated in the base stations within an area. Each base station will bear a code of the area within which it is domiciled; i.e., its *cell*, as illustrated in Figure 2. The radio signal originating from such base stations will be routed with city/area code parameters to disclose the origin of a call via the Cell of Origin (COO). Further binning of the available area codes, as defined by the Nigerian Communications Commission (NCC) [22], like in the case of USA [25], can be made to ensure discrete proximity to the COO of a mobile phone radio information. Thus, for each call placed by a user, the trunk prefix in the trunk code [22] (i.e. the '0' in '043' of 043-805123456, for example) will remain, but the trunk code will be modified to characterise the discrete area in the city from where a call originated.

The hierarchical structure of a cellular network is illustrated in Figure 2 [45]. The structure is formed by connecting the major components like mobile phones, Base stations (BS) and Mobile Switching Centres (MSC). The BS serves a cell which could be a few kilometres in diameter as shown in Figure 2 (a); instead of using a circle to depict an ideal situation, the hexagon is used for convenience. When the cells are grouped together, they form a Cluster as shown in Figure 2 (b). Usually, the number of cells in a cluster is limited by the requirement that the clusters must fit together like jig-saw pieces. The possible cell clusters are the 4-,7-, 12- and 21-cell clusters [45]. The size of a cell can be changed or reduced by splitting the original cell. Figure 2 (c) illustrates how a cell can be split into four; this involves reducing the radius of the original cell by half [45]. As illustrated in Figure 2 (d), all BSs in a cluster are connected to the MSC using land lines. Each MSC of a cluster is then connected to the MSC of other clusters and a Public Switched Telephone Network (PSTN) main switching centre. The MSC stores information about the subscribers located within the cluster and is responsible for directing calls to them [45].

The advantage of these codes is that it will be relative to the specific geographical location of a mobile phone; for instance, if a user leaves *Gwarimpa* for *Nyanya* (two different areas in Abuja, Nigeria), the area code would change and would identify where the caller resides at the time of call. This is also the case for inter-states.

Genuine privacy issues may not be relevant since, as in the current situation, users would be at liberty to either activate or de-activate the Caller ID facility [6].

In security related terminologies, this proposal is inherently a location-based authentication initiative; though it does not comprise all the ingredients of AAA (Authentication, Authorisation and Accounting) [26-28]. However, all the processes of AAA [6] would be a security requirement for the operations of special security agencies. These security agencies and some designated top government functionaries could be permitted by the NCC and the network operators, at the instance of necessary legislations, to operate special mobile numbers and phones that would not reveal these city/area codes.

5. Anticipated challenges

Every technology evolves with its challenges; this is no exception. In this section, the possible challenges that may evolve with this proposal are enumerated, with possible countermeasures spelled out.

5.1 Roaming

Most times, the mobile phone user travels abroad for conferences, trainings, workshops, businesses, health, etc. Most of these users prefer to roam their calling IDs. This technology (if operated in Nigeria only) cannot provide the city codes of the foreign countries (unless it is adopted there or globally). However, except for the case of roaming, the proposed city codes provide well-binned space-time information of a mobile phone user based on city/area codes. The possible effect of roaming on the reliability of the proposed system is analysed via a survey in Appendix A; with encouraging results. The survey showed that, in pragmatic terms, about 1.0% of the targeted population roam their mobile services, and less than 2.25% of this (1.0%) are under the age of 35 (the age range for active cyber offenders). Hence, it would be safe to posit that the likely negative effect of GSM roaming on the proposed LBA as a means of mitigating the incidence of 419 advance fee fraud, and related cyber offences in Nigeria, would be negligible.

5.2 Awareness education

In Nigeria, most users tend to believe that all telecommunications caller numbers not starting with the trunk prefix (zero) is an international call. This has been used to swindle victims more often than not. When this proposal is implemented, most users will face the challenge of adjusting to recognize that all numbers not beginning with the zero prefix are not foreign numbers. It is hoped that a sensitization campaign will be carried out to educate the general public about the change using newspapers, radio, TV stations, posters, etc. The Government at all levels, NCC, Mobile Service Providers (MSPs) and security agencies would have an important role to play in this regard.

5.3 Cloning fraud

This is a high-tech problem that can be perpetrated only by some experts who are capable of knowingly, wittingly or fraudulently obtaining the factory details of a mobile-phone or by monitoring the radio characteristics of a particular mobile phone for a long time. Cloning fraud occurs when the factory-set Electronic Serial Number (ESN) and telephone Mobile Identification Number (MIN) has been dubbed and used to programme a different phone so that when the legal, as well as illegal (cloned), user places a call, the ESN/MIN of the legitimate mobile will be transmitted [29, 25]. The transmission of similar ESN/MIN from different mobile nodes is already known [29] and described as a *Sybil* attack in, for example, wireless sensor networks [31-35], and several solutions have been suggested [36-40]. It will be easy to identify the location from which the fraudulent user calls when the proposed method is adopted, since the city/area codes would be different. This can easily isolate the legitimate user from the illegal user. Meanwhile, for cell phone cloning fraud, the cellular equipment manufacturing industry has deployed authentication systems that have proven to be a very effective countermeasure [30].

5.4 Immunity/Security of special security agencies and authorised government functionaries

It may be delicate to always reveal the space-time information of a security professional, such as the agents of State Security Service (SSS). These security agents and some designated top government functionaries could be permitted by the NCC and the MSPs, at the instance of necessary legislations, to operate special mobile numbers and phones that would not reveal these city/area codes.

5.5 Man-in-the-middle and rogue base-station attacks

The man-in-the-middle (MitM) attack involves intercepting a call and re-routing it through a third party to the receiver at the other end, such that both the original source and the sink do not know that the link is compromised. This can be tackled by authenticating the Mobile User (MU) and a Home e-Node B (HeNB or LTE Femtocell) from a contractual proxy-signature already established between the HeNB and OAM (Operation, Admission and Maintenance) [41]. A rogue base station may lead to a Denial of Service (DoS). Meanwhile, DoS due to a rogue base station has been discovered and solution proffered in [42] including impersonation [43].

5.6 Compatibility with future evolutions

LTE-A Rel-10 and beyond, is not a new radio-access technology but the *evolution* of LTE to further improve the performance [43]. This evolution inherited all the Rel-8/9 functionalities with additions such as carrier aggregation, enhanced multi-antenna support, improved support for heterogeneous deployments, and relaying [43]. The Rel-9 uses OTDOA for uplink and E-CID (Enhanced-Cell ID) for both uplink and downlink [24]. The E-CID positioning algorithm, in addition to the serving eNB (in other words the radio cell) and the broadcast cell ID which was defined in LTE Rel.8, the information such as propagation delay calculated from the difference in timing of signal transmission and reception and the Angle of Arrival (AoA), are utilised to estimate the MU position [21]. For other lower standards, the proposed technology would comfortably fit in.

5.7 Replacement for other positioning algorithms

This algorithm may rather be seen as the primary algorithm to which any other possible geographical positioning algorithm can be appended. For instance, the use of GPS can be added to the city code algorithm. After all, the Rel-9 was defined to involve assisted-GPS (A-GPS), OTDOA and E-CID [24].

6. Conclusion

The degree of insecurity occasioned by fraudulent practices has been an issue of great concern economically, especially as it relates to foreign direct investments and dealings with other international partners. Apart from the economic costs to the nations and individuals, it has also been an image problem for Africa, using Nigeria as a case study, in various international fora. This paper examines possible technological means of addressing this problem. The suggested solutions, though tailored specifically for the Nigerian environment, are applicable to all countries with similar situations.

The paper used the results of surveys involving field trips to Nigeria in November 2013 and 2015/2016, among other resources, to look at the cyber security problems in Nigeria to arrive at some promising solutions. It was realised that most previous efforts at countering cyber and other fraud-related crimes in Nigeria depended mainly on the use of legal instruments. It was also realised that the 419 Scam is a major contributor to Nigeria's third position in the world, with 5.7% of cybercrime perpetrators.

The main technological proposal to tackle this problem is to further digitise the GSM country code into city/area codes which will be transmitted along with caller IDs to reveal the location of the caller, as is currently done with fixed telephones. Anticipated challenges, which include the possible impact of mobile communication roaming on the efficacy of the proposed system, as highlighted in Appendix A, were found to be negligible.

Appendix A. Survey: Effect of GSM roaming on location based authentication

Two surveys were conducted, with field trips to Nigeria; partially in November 2013 and December/January 2015/2016. The approaches included the use of questionnaires, structured interviews and examination of official documents; using direct personal contact, email and phone calls. The data obtained from the security agencies (NP, SFU, NFIU, EFCC and NCC) and individual targets, among others, facilitated the discussions on cybersecurity in Section 3 and Appendix A [1]. Details of the survey on GSM roaming are now presented in this Appendix.

Due to the lack of cooperation by the MSPs which frustrated the completion of the survey in 2013, it was decided that random samples of individuals be used from a population of (about 250) Nigerians of all designations from all parts of the country and beyond. The data was mainly generated using a questionnaire attached to the structured interview sample questions for GSM mobile services. The results of the survey are presented in Figures A.1 and A.2.

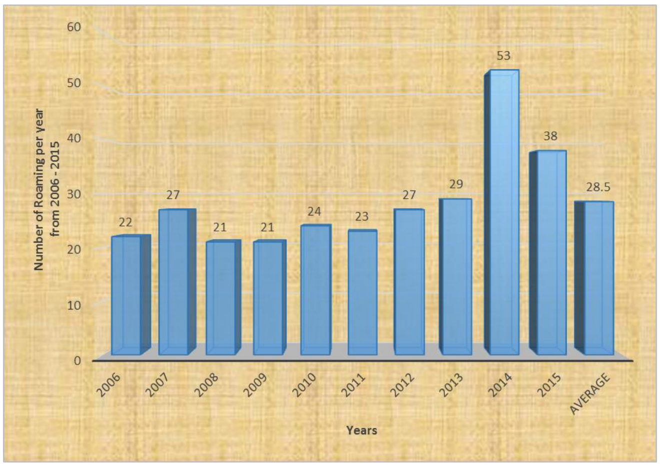


Figure A.1. Total and Average Annual Roaming Statistics in a Decade

A.1 Survey Results Analyses

From Figure A.1, it is obvious that the members of the targeted population who roam their mobile services are in the region of 10%. Bearing in mind the fact that part of the roaming incidence is at the discretion of the MSPs rather than the subscribers, personal interactions also authenticated that the roaming subscribers are not only less than 10% of the population, their actual usage of the roamed services is also much less than 10% (i.e., 10% of 10% = 0.1 x 0.1 = 0.01 = 1.0% of the population); i.e., less than 1.0% effective roaming.

The above result is not an exaggeration because, in practice, most of those who roam their mobile services only use them to view calls; to enable them use other cheaper facilities to contact their callers in cases of important calls. This is due to the factual belief that roamed services are extravagantly costly. Figure A.2 illustrates the fact that the number of those who roamed their mobile services only once in a year is conspicuously much higher than those who roamed twice or more.

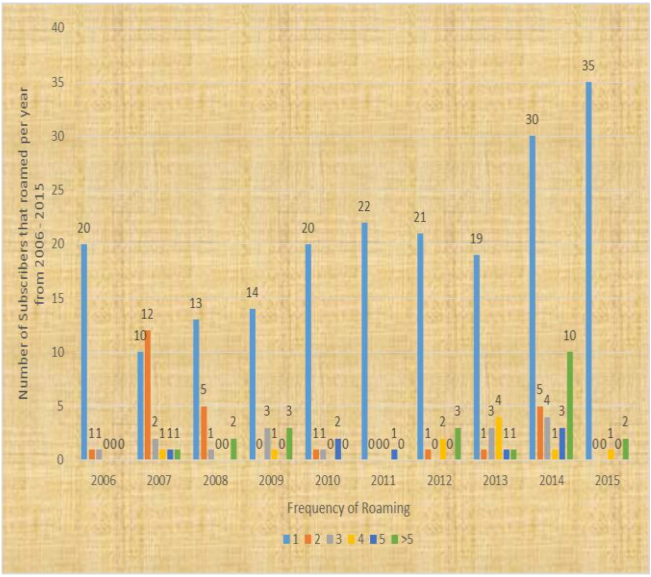


Figure A.2. Annual Roaming Frequency

From the above statistics, it cannot be safely posited that the incidence of effective roaming is on the rise because, of recent, more roaming is done at the instance of the MSPs. It is noteworthy, that there were abrupt hikes in the number of roaming subscribers in 2014 and 2015. Firstly, these could be explained by two possible reasons: Firstly, there were more roaming at the instance of the MSPs as a marketing strategy to make more money at all costs; secondly, these might be connected with the uncertainties associated with the general elections earlier scheduled for 14th February 2015 – it was postponed and later held on 28th March 2015. This second reason is informed by the fact that most of the roaming within the time frame was concentrated in the last quarter of 2014 and first quarter of 2015; with a good number of the affected individuals being politicians.

From the foregoing, it could be deduced that there remained a culture of lukewarm attitude towards roaming among Nigerians, throughout the decade under review. It is also very impressing to observe that about less than 2.25% of the roaming subscribers were under the age of 35; data from and discussions with the SFU/EFCC indicate that the effective age bracket for most cyber offenders in Nigeria is from 20 – 35 years. Thus, it could be concluded that, in pragmatic terms, about 1.0% of the targeted population roam their mobile services, and less than 2.25% of this are under the age of 35. Hence, it would be safe to posit that the likely negative effect of GSM roaming on the proposed LBA as a means of mitigating the incidence of 419 advance fee fraud, and related cyber offences in Nigeria, would be negligible.

Acknowledgments

The role of the Petroleum Technology Development Fund (PTDF, Nigeria) for sponsoring the main PhD Programme, which produced this paper, is hereby acknowledged. The same is true of the Nigerian Army which approved the programme. The authors also appreciate the contributions of the various staffs and departments of the School of Engineering and Informatics, University of Bradford, UK.

References

[1] ADEKA, M.I.U., SHEPHERD, S.J. and ABD-ALHAMEED, R.A. (Ongoing: 2011-) Cryptography and computer communications security: extending the security perimeter through a web of trust. *PhD Thesis Draft, School of Engineering and Informatics, University of Bradford, Bradford (UK).*

[2] OTTIS, R. and LORENTS P. (2010) Cyberspace: Definition and implications. *Proceedings of the 5th International Conference on Information Warfare and Security.*

[3] THOMAS, S. (2013) *Technobiophilia: Nature and Cyberspace*, A&C Black**.**

[4] ROUSE, M. (2007). *Peripherals Glossary*. Available: http://whatis.techtarget.com/definition/digitization. (Accessed: Sep. 28. 2014)

[5] MOORE G.E (1965) "Cramming more components onto integrated circuits," ed: McGraw-Hill New York, NY, USA.

[6] ADEKA, M., SHEPHERD, S. and ABD-ALHAMEED, R. (2013) Extending the security perimeter through a web of trust: The impact of GPS technology on location-based authentication techniques. In *Proceedings of the Fifth International Conference on Internet Technologies and Applications (ITA 13)*, pp. 465-473,.

[7] ASLAM, H.D., AZHAR, M.S., Yasmeen, K.H., FARHAN, M. BADAR, M. and HABIB, A. T. (2012) Effects of globalization on developing countries. *Journal of American Science,* vol. 8.

[8] Core ICT Indicators-ITU. Available: http://www.itu.int/pub/D-IND-ICT_CORE-2010/en ed, 2005. (Accessed: Sep. 28. 2014)

[9] HADNAGY, C. (2010) *Social engineering: The art of human hacking*: John Wiley & Sons.

[10] CHAWKI, M. (2009) Nigeria tackles advance fee fraud. *Journal of Information, Law and Technology,*.

[11] EHIMEN, O. and BOLA, A. (2010) Cybercrime in Nigeria. *Bus Intelligence J,* vol. 3, pp. 93-98,.

[12] ASHAOLU, D. (2011) Combating cybercrimes in nigeria. *Upcoming cyberlaw textbook,*.

[13] EFCC, (September 2013) EFCC annual report.

[14] N.P. (SFU), (2014) Fraudulent crime statistics (EFCC/NFIU) - 2012 - 2014.

[15] *Internet World Statistics,* Available: http://www.internetworldstats.com/af/ng.htm. (Accessed: Sep. 28. 2014)

[16] *Nigerian Communications Commission*. Available: http://ncc.gov.ng/index.php?option=com_content&view=article&id=125:subscriber-statistics&catid=65:industry-information&Itemid=73. (Accessed: Sep. 28. 2014)

[17] RINNE, M. and TIRKKONEN, O. (2010) LTE, the radio technology path towards 4G. *Computer Communications,* vol. 33, pp. 1894-1906.

[18] AKYILDIZ, I.F., GUTIERREZ-ESTEVEZ, D.M. and REYES, E. C. (2010) The evolution to 4G cellular systems: LTE-Advanced. *Physical Communication,* vol. 3, pp. 217-244.

[19] SAYED, A.H., TARIGHAT, A. and KHAJEHNOURi, N. (2005) Network-based wireless location: challenges faced in developing techniques for accurate wireless location information," *Signal Processing Magazine, IEEE,* vol. 22, pp. 24-40.

[20] GHOSH, A., RATASUK, R., MONDAL, B., MANGALVEDHE, N. and THOMAS, T. (2010) LTE-advanced: next-generation wireless broadband technology [Invited Paper]. *Wireless Communications, IEEE*, vol. 17, pp. 10-22.

[21] ABETA, S. (2010) Toward LTE commercial launch and future plan for LTE enhancements (LTE-Advanced). In *Communication Systems (ICCS), 2010 IEEE International Conference on*, pp. 146-150.

[22] *Technical Standards: National Numbering Plan*. Available: http://www.ncc.gov.ng/index.php?option=com_content&view=category&id=75&Itemid=102 (Accessed: Oct. 2, 2013)

[23] *Country Codes, Phone Codes, Dialing Codes, Telephone Codes, ISO Country Codes*. Available: http://countrycode.org/ (Accessed: Oct. 02, 2013)

[24] JOHN, M. (2011) Location services part 2: lte release 9 features. *LTE University*.

[25] *Area Code History*. Available: http://www.area-codes.com/area-code-history.asp (Accessed: Oct. 2, 2013)

[26] JAROS, D. and KUCHTA, R. (2010) New location-based authentication techniques in the access management. In *Wireless and Mobile Communications (ICWMC), 2010 6th International Conference on*, pp. 426-430.

[27] SONG, Z., Li, Z. and DOU, W. (2003) Different approaches for the formal definition of authentication

property. In *Communications, 2003. APCC. The 9th Asia-Pacific Conference on*, 2003, pp. 854-858.

[28] HE, R., YUAN, M., HU, J. ZHANG, H. KAN, Z. and MA, J. (2003) "A novel service-oriented AAA architecture," in *Personal, Indoor and Mobile Radio Communications, 2003. PIMRC, 14th IEEE Proceedings on*, 2003, pp. 2833-2837.

[29] KOU, Y., LU, C.T., SIRWONGWATTANA, S. and HUANG, Y.P. (2004) Survey of fraud detection techniques. In *Networking, sensing and control, 2004 IEEE international conference on*, , pp. 749-754.

[30] *Cell Phone Fraud*. Available: http://www.fcc.gov/guides/cell-phone-fraud (Accessed: Oct. 2, 2013) Y.

[31] DEMIRBAS, M. and SONG, Y. (2006) An RSSI-based scheme for sybil attack detection in wireless sensor networks. In *Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks*, pp. 564-570.

[32] JDOUCEUR, J.R. (2002) The sybil attack. In *Peer-to-peer Systems*, ed: Springer, pp. 251-260.

[33] SSU, K.F., WANG, W.T., and CHANG, W.C. (2009) Detecting sybil attacks in wireless sensor networks using neighboring information. *Computer Networks*, vol. 53, pp. 3042-3056,.

[34] YIN, J. and MADRIA, S. K., (2007) Sybil attack detection in a hierarchical sensor network. In *Security and Privacy in Communications Networks and the Workshops. SecureComm. Third International Conference on*, pp. 494-503.

[35] ZHANG, Q., WANG, P., REEVES, D.S. and NING, P. (2005) Defending against sybil attacks in sensor networks. In *Distributed Computing Systems Workshops, 2005. 25th IEEE International Conference on*, , pp. 185-191.

[36] YU, H., KAMINSKY, M., GIBBONS P.B., and FLAXMAN, A. (2006) Sybilguard: defending against sybil attacks via social networks. In *ACM SIGCOMM Computer Communication Review*, pp. 267-278.

[37] KHALIL, I., BAGCHI, S., ROTARU, C.N. and SHROFF, N.B. (2010) UnMask: Utilizing neighbor monitoring for attack mitigation in multihop wireless sensor networks. *Ad Hoc Networks*, vol. 8, pp. 148-164.

[38] LEVINE, B.N., SHIELDS, C., and MARGOLIN, N.B. (2006) A survey of solutions to the sybil attack. *University of Massachusetts Amherst, Amherst, MA*,.

[39] LV, S., WANG, X., ZHAO, X. and ZHOU, X. (2008) Detecting the sybil attack cooperatively in wireless sensor networks. In *Computational Intelligence and Security, CIS'08. International Conference on*, , pp. 442-446.

[40] DANEZIS, G. and MITTAL, P. (2009) SybilInfer: Detecting sybil nodes using social networks. In *NDSS*.

[41] CAO, J., MA, M., LI, H. and ZHANG, Y. (First Quarter 2014) A Survey on security aspects for LTE and LTE-A networks. *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*, 16, no. 1 283–302.

[42] BARBEAU, M. and ROBERT, J.M. (2006) Rogue-base station detection in WiMax/802.16 wireless access networks. In *Annales des télécommunications*, pp. 1300-1313.

[43] BARBEAU, M., HALL, J. and E. KRANAKIS, (2006) Detecting impersonation attacks in future wireless and mobile networks. In *Secure Mobile Ad-hoc Networks and Sensors*, ed: Springer, pp. 80-95.

[44] PARKVALl, S., FURUSKÄR, A. and DAHLMAN, E. (2013) Evolution of LTE towards IMT-Advanced [Online]. Available: http://www.ericsson.com/res/docs/2013/evolution-of-lte-towards-imt-advanced.pdf (Accessed: Oct. 2, 2013)

[45] LEE, W.C. *Mobile cellular telecommunications: analog and digital systems*: McGraw-Hill Professional, 1995.