International Journal of Advanced Computer Technology (IJACT)

ISSN:2319-7900

A SYSTEM FOR ASSESSING THE GEOLOCATION OF INTERNET USERS IN A CDMA-EVDO NETWORK

Ebot Ebot Enaw
University of Yaounde I, Cameroon
National Advanced School of Engineering
Department of Computer Sciences

Abstract

Given that our society is increasingly dependent on Internet in almost every aspect of our daily life, it has become a major driver of economic growth.

Due to the fact that Wireless communication can be deployed fast and easily, it became the most popular technology for Internet access.

Unfortunately, cybercriminals also use wireless technology to hack into systems and carry out illegal activities. In an effort to prosecute these cybercriminals, Law enforcement have to identify and locate them.

This paper presents a system we developed to enable us obtain a good estimate of the location of cybecriminals that access Internet through a CDMA (EVDO) network.

Keywords: *geolocation, AOA,TDOA,CDMA..*

1 Introduction

In recent years, wireless technology has become the best way to provide Internet to customers. With the transition from 2G to 3G and 4G, Telco are now able to provide broadband access to their customers easily. CDMA-EVDO which falls under the 3G technology is increasingly adopted by Telco especially the one this article is based on. As the number of cybercrimes is soaring over time, Law enforcement have to take appropriate measures to identify and localize cybercriminals. Numerous methods have been developed to get the location of a terminal in a wireless network namely: Angle of Arrival (AOA) and Time Difference of Arrival (TDAO).

The aim of this paper is to present an approach for the development of a system to calculate an estimate of the location of a CDMA-EVDO terminal, within a CDMA network.

2 Related work

Some research have been done on topics related to this issue namely [1] that in an effort to improve the passive geo-location of grounded target performed by surveillance aircraft, develops a mathematical model to relate the direction finding angle to the position of the terminal on earth and also provided a measurement matrix to evaluate the accuracy.

[2] proposes an Adaptative Extended Kalman Filter (AEKF) that implements a moving target tracking algorithm using the measurements signal of Time Difference of Arrival (TDOA) and Frequency Difference of Arrival (FDOA) and updates the noise covariance at each measurement.

[3] presents a hybrid AOA/TDOA mobile station estimation method. The methodology adopted by the authors in this article consists of: firstly presenting the AOA and TDOA algorithm and challenges, then a mathematical model for an hybrid AOA/TDOA method and its linearized model based on Taylor series was derived and finally the performance of TDOA and AOA/TDOA systems were compared when the client has access to minimum LOS (Line of Sight) signal.

[6] first conducts a thorough mathematical analysis of the distance-difference method of localization and then establishes formal properties for an optimal location process in an Euclidian plane as well as in a simple polygon.

While [1], [2] and [3] present a specific method of geo-location mostly from a theoretical point of view, our article first conducts a comparative study of these methods based on theoretical and practical criteria, then optimizes the selected method with the mathematical properties derived in [6] and finally proposes a practical approach to build a system which provides a better estimate of the position of a Mobile station in a CDMA network.

This paper is intended to help developing countries that can't afford branded geo-location systems due to budget constraints, to develop customized geo-location systems using the methodology and practical approach outlined, and as such make savings which can be used to develop other sectors of the economy.

3 Research problem

Because wireless networks are now the primary means by which people access the Internet especially in Africa, it raises a particular interest for Governments and Law Enforcement especially for the geo-location of cybercriminals. In fact, in [5] we developed an application that uses data gathered from the CDMA network components (AAA, NAT table, Customer Database), to obtain the identity of a cybecriminal based on its IP address as well as the ID of its mobile station which then serves to get the base station through which it is connected. However, because a base station can cover a wide range that can go up to 1.000.000 m^2 it is quite difficult to identify a cybercriminal in real time especially in a city where the population density is high.

In an effort to address the search area problem, in this paper we develop a system that provides a better estimate of the geo-location of a mobile station, by limiting the search area and as such hastens investigation.

4 CDMA

Code Division Multiple Access (CDMA) is a technology that uses a form of transmission known as Direct *Sequence Spread Spectrum (DSSS)*. All users transmit in the same wide-band chunk of spectrum. Each user's signal is spread over the entire bandwidth by a unique spreading code. At the receiver, the same unique code is used to recover the signal. The use of CDMA spread spectrum is a powerful principle and using this technique, it is possible to transmit several sets of data independently on the same carrier and then recover them at the receiver without mutual interference. It provides so many advantages including: immunity to interference and jamming, and the possibility for many users to access the same frequency band at the same time.

Since the first version CDMAone, other versions were released over time namely CDMA2000 and WCDMA.

CDMAone is a 2G network that can provide data rate of up to 14.4 kbps. Later, to support the third generation services as specified by ITU, CDMA2000 was released. The most popular types of CDMA2000 networks are EVDO-REVA that achieves an average data throughput on loaded networks of 600-1400 kbps in the forward link and 500-800 kbps in the reverse link and EVDO-REVB that can deliver through the aggregation of multiple carriers, up to 14.3 Mbps in the downlink and 5.4 Mbps in the uplink.

WCDMA (Wideband Code Division Multiple Access) is a mobile technology that improves upon the capabilities of current GSM networks that are deployed around the world. It was specified by the 3GPP to provide third generation services. Combined with HSPA+, it can deliver data at up to 42.2 Mbps in the downlink and 11.5 Mbps in the uplink.

5 CDMA Network Components

As depicted in the figure below, the CDMA network is made up of several components namely:

- The Mobile Station (MS): It is the terminal used by the client to initiate and receive calls and data ;
- The Base Transceiver Station (BTS): It transmits and receives radio signals, realizing communication between the radio system and the mobile station ;
- The Base Station Controller (BSC): It implements several functions such as BTS control and management, call connection and disconnection and mobility management ;
- Mobile Switching Center (MSC): It implements the service switching between the calling and called subscribers. One MSC is connected to multiple BSCs. The MSC can also be connected to the PSTN, ISDN or other MSCs ;
- Packet Data Service Node (PDSN): The PDSN implements the switching of packet data services of mobile subscribers. One PDSN can be connected to multiple PCFs. It provides the interface between the radio network and the packet data network ;
- Visitor Location Register (VLR): It is a database used to store the subscriber information of all the MSs in its local area which can be used to establish the incoming/outgoing call connections, to support basic services, supplementary services and mobility management ;
- Home Location Registry (HLR): It is a database for mobile subscriber management, the HLR (Home Location Register) is responsible for storing subscription information (telecom service subscription information and subscriber status), MS location information, IMSI, etc ;
- AAA (Authentication Authorization Accounting) server: It authenticates users on a network and based on the policy and the data of the billing system, it authorizes users access to specific services. It also logs events related to the interaction between the mobile station and the network

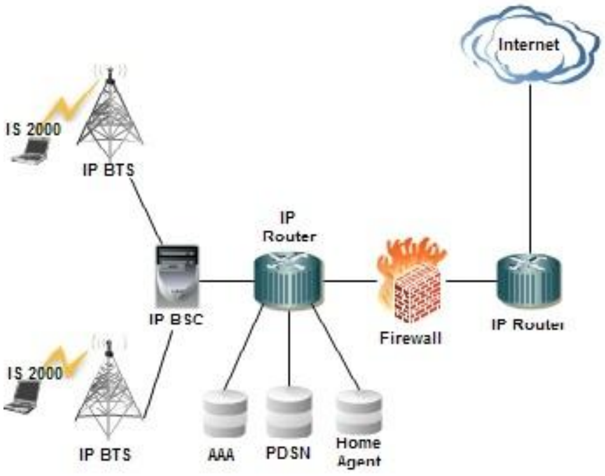

Figure 1: Architecture of the network

6 Some Geolocation techniques in Wireless Networks

All geolocation techniques fall under two main categories:

- Self-positioning: This category encompasses all geolocation methods whereby the mobile station assesses its position based on data evaluated through its interaction with the base transmitter station. Self-positioning methods usually require that additional hardware should be integrated into existing handsets.
- Network positioning: This category encompasses all geolocation methods whereby receivers at known

ISSN:2319-7900

location on the network together compute the location of the mobile transmitter using the measurement of the distance or direction from each of the receiver.

Though, self-positioning methods can provide more accuracy than network positioning, they induce extra-cost and higher weigh due to additional hardware. Furthermore, self-positioning methods depend heavily on the mobile station and this makes it difficult to implement for investigation purposes, where total independence from the mobile station is needed. In the subsequent sections, we will study the main geolocation methods.

6.1. Angle of Arrival

With this method, the receiver (BTS) measures the direction of arrival (DOA) of the received signals from the target transmitter (MS) using directional antenna or antenna arrays. Thus a single DOA measurement restricts the source location along a line in the estimated DOA. If at least two such DOA estimates are available from two antennas at two different locations, the position of the signal source can be located at the intersection of the lines of bearings from the two antennas as depicted in the figure below. Usually multiple DOA estimates are used to improve the geolocation accuracy.

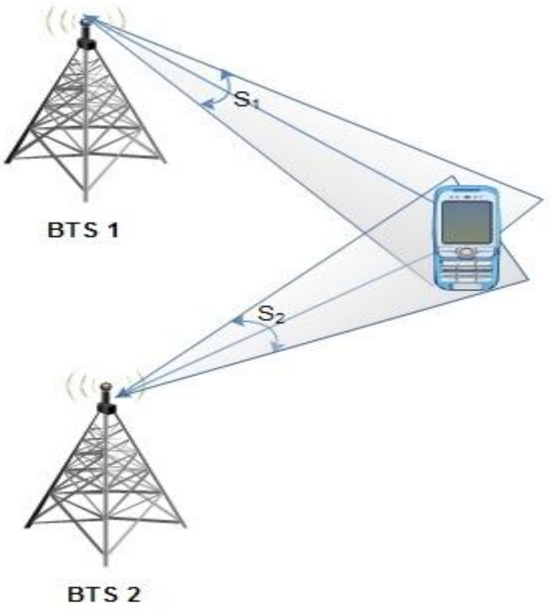

Figure 2: AOA technique

Although this method can provide good results it has some setbacks including:

- if the Line of Sight (LOS) signal is blocked, and a DOA of a reflected or scattered signal is used, this will induce large error. This is a major issue especially in urban environment where too many obstacles (wall, three, objects) exist.
- This method requires antenna arrays which are quite costly and require to be ruggedly installed or continuously calibrated because a change in the position of the array may result in a large error in the assessment of the location of a mobile station.

6.2. Time of Arrival method

This method exploits the fact that it is established that a signal travels at the speed of 3x10^{-8} m/s in air. Thus, if the time the signal was emitted and the time the signal is received are known, then it is possible to evaluate the distance between the receiver and the transmitter. This can be done by measuring the time in which the mobile responds to an inquiry sent from the base station. The total time elapsed from the moment the command is transmitted to the moment the mobile's response is received, is the sum of the round trip signal delay and any processing delay within the mobile station. If the processing delay for the desired response within the mobile is known with sufficient accuracy, it can be subtracted from the total measured time to obtain the total round trip delay which will then be used to calculate the distance $R=(3x10^{-8})xT/2$ where T represents the total round trip delay. Moreover if this process can be implemented on three base stations, then, the position of the mobile station can be calculated by the triangulation method which basically consists of finding the intersection zone of the three circles. In fact, since we have an estimate of the distance r between the mobile station and a base station, the search area where the MS is supposed to be is the circle of radius r centered at that BTS. Thus, with three BTS, we have three circles as depicted in the figure below and the triangulation method then consists of finding the intersection zone of these circles.

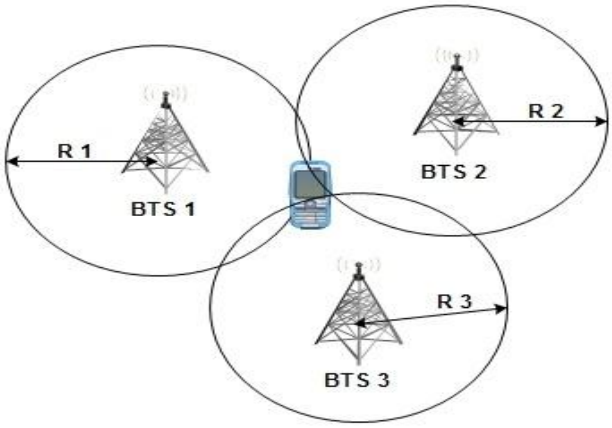

Figure 3: TOA technique

However, this method also has some setbacks including:

- Since handsets differ in technical design, it is quite difficult to obtain an accurate value of the processing delay;

- In the absence of Line of Sight (LOS), it is quite difficult to reduce errors induced by signal reflections.

6.3. Time difference of Arrival method

This method consists of evaluating the difference in the arrival times of the signal from the mobile station at multiple base stations. It is usually accomplished by taking a snapshot of the signal at a synchronized time period at multiple base stations. This results in several hyperbolas, as depicted in the figure below, and to which the intersection of is the location of the mobile station. This method offers some benefit over others including:

- Immunity against time errors as signals experience reflections, the time errors may be annihilated due to the fact that source of reflections affects all the base stations.

- It does not require knowledge of the transmit time by the mobile station.

However, this method requires the base stations to be tightly synchronized.

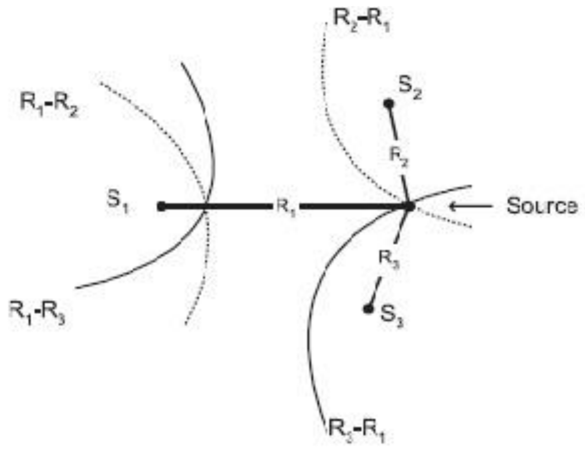

Figure 4: TDOA technique

6.4. Hybrid AOA/TDOA method

With this method, multiple base stations receive the signal, and the MS position is calculated by combining AOA estimates from each base station and TDOA estimates between multiple base stations. AOA estimates are made using an adaptive array. Times of signal arrival are measured at each base station and are time stamped with a GPS time reference to determine time-difference of arrival estimates. The impact of multipath can be minimized by using highly directional adaptive antennas that offer spatial filtering.

The hybrid method becomes more advantageous in situations where users only have access to limited BSs, or the MS cannot receive reliable signals from some BSs.

6.5. Fingerprinting method

As it is established that the signal propagation is extremely site-specific because of its dependence on the field and intervening obstacles, the multipath structure of the channel is unique to every location and can be considered as a fingerprint or signature of the location if the same RF signal is transmitted from that location. In this light, this method consists of recording the signature of every places in a database and comparing the signature of the place where the target is located to the signatures stored in the database in order to evaluate the position.

Though this method can provide reliable results, its implementation at a large scale (country) may be quite difficult because the fingerprints of every place should have been recorded.

7 Our Solution

After studying the main geolocation methods as described in the previous sections, we arrived at the conclusion that in our context, the Time Difference of Arrival (TDOA) method is more appropriate firstly because it doesn’t require any modification on the mobile station and secondly, the errors induced by reflections are almost completely canceled. However, addressing the issue of developing a practical system for assessing the geolocation of a mobile station requires that we develop a methodology.

7.1. Methodology

In order to develop our system, we adopted the following methodology:

1. Identify all the base stations of the target Telco with their GPS coordinate and design a Geographic Information System to manage these data ;

2. Develop a module that will access the database of the base station controller to identify the base station with which a mobile station is communicating as well as the characteristics of the link (power, time delay) between them and the mobile station ;

3. Develop a module that will select the best suited base stations on which to apply the Time Difference of Arrival method ;

4. Develop a module that will process the data coming from the selected base stations using the TDOA method.

7.2. Description of the system modules

With regard to the methodology presented in the previous sections, our system will be made up of five (05) modules as depicted in the figure below. These modules will be described in subsequent sections.

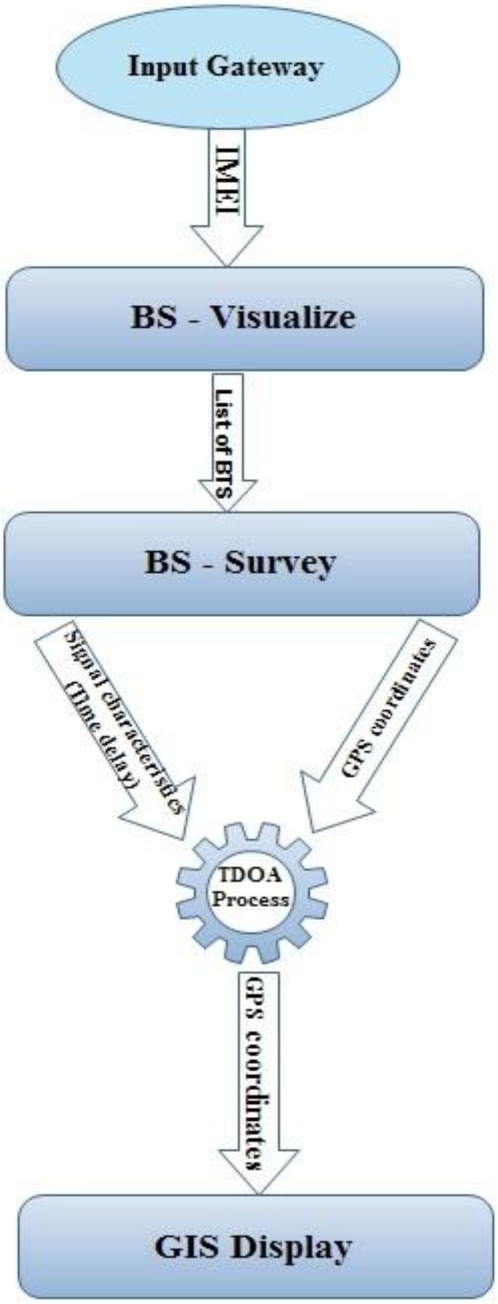

Figure 5: Architecture of the system

7.2.1 Geographic Information System

This module has two main features namely:

- It provides an Interface whereby the system administrator can enter the GPS coordinate of different base stations as well as their coverage radius. These data are then stored in a relational database ;
- It provides a way to interact with Google map. The base stations that are indexed in the database are displayed in the map as little symbols and a user can click on these symbols to display all the information related to the base station.

7.2.2 Input Gateway

This module serves as a gateway to the application. It implements a webservice (SOAP) that has as parameter the IMEI of the target mobile station and passes to the application for processing. This module is necessary firstly because our geo-location system can have many applications including locating E-911 callers, and cybercriminals tracking. Thus, as this system will interact with several other applications which may use different technologies, it should be interoperable with all these technologies. That's why we used the Service Oriented Architecture Protocol (SOAP).

Moreover, it is worth mentioning that as this geo-location system is a continuation of the Internet traffic record platform described in [5], which outputs several data including the IMEI of a targeted mobile station, this module will be the interface between that platform and the geo-location system.

7.2.3 Base station visualizer

This module is aimed at interacting with the base station controller databases in order to determine the list of base station with which a particular mobile stations is connected as well as the characteristics of the link (power of the signal, time delay, etc) between each of these base station and the mobile station. In this light, this module connects to the BSC and query them through the IMEI of the target mobile station.

7.2.4 Base station survey

Given that the accuracy of the TDOA method depends heavily on the dispersion of the base station, as well as the reliability of the link between the mobile station and the base station, it is critical to select base stations on which to apply the TDOA algorithm. [6] established mathematical conditions that the dispersion of the base stations should satisfy in order to improve the accuracy of the results. This module implements an algorithm that based on the list of base stations with which the mobile station communicates, their GPS coordinates and the characteristic of their respective link to the MS, selects the base station that will be used in the TDOA algorithm so as to minimize the error.

7.2.5 TDOA processor

This module takes as input the GPS coordinates of the base stations selected by the *base station survey* module, the characteristics of the link (delay time) between the mobile station and the selected BS provided by the *base station visualizer* module and then processes them using the TDOA algorithm to obtain an approximation of the GPS coordinate of the mobile station.

7.3 Technical environment

To develop our solution we used:

- A server with the following characteristics: 16 GB RAM, 1To Hard disk, Intel Xeon 1.87Ghz *16
- **Netbeans 7.3**: Netbeans is a popular free IDE (Integrated Development Environment) that supports many languages like Java and PHP ;
- **Java** and **Tomcat 7.0.34.0**

8 Some Results

In order to assess our system, we carried out the following test. We went to five (05) different locations and got connected to the network using a Huawei EC 306 RevB mobile station, then using a GPS we measured the exact coordinates of our position as well as those of three base stations with which the mobile station was communicating. Using our system, we then processed the BS coordinates as well as the signal characteristics collected from these BS to obtain an estimate of the position of the MS that we compared to the exact one previously obtained from the GPS. The results of this test are presented in the following table. The first number represents the latitude and the second one represents the longitude.

Table 1: Results

N°	BTS1	BTS2	BTS3	Exact MS coordinates	Calculated MS coordinates	Gap
1	3°,52’,43.231” 11°31’32.635”	3°,52’,44.538” 11°31’20.083”	3°,52’,38.147” 11°31’32.547”	3°,52’,41.915” 11°31’29.257”	3°,52’,42.024” 11°31’28.292”	15 m
2	3°,52’,43.231” 11°31’32.635”	3°,52’,54.945” 11°31’25.305”	3°,52’,44.538” 11°31’20.083”	3°,52’,44.699” 11°31’36.724”	3°,52’,45.808” 11°31’36.038”	12.5m
3	3°,53’,10.977” 11°31’49.801”	3°,53’,21.659” 11°32’10.566”	3°,53’,31.073” 11°31’49.297”	3°,53’,11.966” 11°31’09.683”	3°,53’,10.831” 11°32’07.301”	9m
4	3°,51’,20.449” 11°31’19.139”	3°,51’,44.435” 11°30’56.779”	3°,51’,55.272” 11°31’18.769”	3°,51’,41.016” 11°31’16.609”	3°,51’,40.500” 11°31’15.651”	10.36 m
5	3°,43’,56.548” 11°32’04.410”	3°,42’,35.149” 11°32’03.033”	3°,42’,53.498” 11°32’47.610”	3°,43’,16.354” 11°32’13.913”	3°,43’,17.896” 11°32’14.387”	14.2m

From these data, we note that the average gap between the positions calculated using our system and the real position obtained using the GPS is 14.3m which means the law enforcement will have to search for the cybercriminal in an area of π x $(14.3)^2$ m^2 that corresponds to the area represented by the circle centered at the calculated position (provided by our system) and of radius 14.3m which represents the gap. To identify the cybercriminal in this space, law enforcement will use forensic tools to obtain the Mobile Equipment ID (MEID) of all terminals, which is unique for each terminal, located in the target area and compares the obtained MEIDs to the MEID of the terminal of the target cybercriminal obtained through the system developed in [5]. The MEID in the target area that matches that obtained through the system developed in [5] is that of the cybercriminal in question.

Our system therefore provides a practical cost-effective approach for tracking and locating cybercriminals. This will definitely hasten investigations since the coverage area to be searched by law enforcement is reduced by more than 90%.

9 Conclusion and future work

The ever growing importance of ICT/Internet in our daily life, coupled with the fact that wireless communication have become the most popular transmission technology used by Telcos, by default, it has also become one of the most popular means by which cybercrimes are conveyed. The results obtained in [5] provided us with the identity of the cybercriminal. This information doesn’t enable law enforcement to track and arrest the cybercriminal in question. For this to happen it is necessary to obtain the geo-location of the cybercriminal in real time, which is the objective of the current paper, which extends the results obtained in [5] by providing an estimate of the geolocation of the cybercriminal in real time. In order to build our geo-location system, we first

ISSN:2319-7900

analyzed and compared the different geo-location methods including TOA, AOA and TDOA, then from this analysis it became apparent that in our context, the most appropriate method is the TDOA method. We then developed an application comprising five (05) modules that collect data from network equipment and process them using the TDOA algorithm optimized with the mathematical properties derived in [6] to obtain an estimate of the position of the target mobile station. Since our system can interact with other applications like the E-911 calls management platform, interoperability was a particular concern that was addressed in its design using SOAP webservices in the *Input Gateway* module. In order to evaluate the performance of our system, we carried out a series of test which revealed that the average error was around 14.3m.

Although this error is quite acceptable, it might be reduced by coupling the TDOA method to another approach like the fingerprinting method. Thus, future work can include the development of a mathematical model to assess the way electromagnetic wave propagate in a particular area so as to improve the accuracy of the position.

References

[1] Kimberly N.Hale, "Expanding the use of time/frequency difference of arrival geolocation in the Department of Defense" in *RAND Graduate School*, 2012.

[2] Dongkyun Kui, Jihyun Tha and Kwanho Yon, "Adaptative extended kalman filter based geolocation using TDOA/FDOA" in *International Journal of Control and Automation*, 2011.

[3] A.Boumandan, T.hu, J.Nielsen, G.lachapelle, "Practical results of hybrid AOA/TDOA geolocation estimation in CDMA wireless networks" in *IEE*, 2008.

[4] Muhammad Aatique, "Evaluation of TDOA techniques for position location in CDMA systems" in *Thesis of Virginia Polytechnic Institue*, 1997.

[5] Ebot Ebot Enaw, "A practical approach to build a system for the collection and analysis of Internet traffic record for law-enforcement" in *International Journal of Advanced Technology*, 2014.

[6] Xiaochum Xu, "On basic properties of localization using distance-differences" in *Information Fusion*, 2008.

Biography

Dr. EBOT EBOT ENAW obtained his B.Eng hons degree from Liverpool University in Electronic Engineering in 1989. He later obtained an M.Eng degree in Telecommunication Engineering from The University of Manchester England in 1991. He returned home where he was recruited in the University of Yaounde I, as an assistant lecturer. He pursued his university studies and obtained a PhD in Computer Sciences from the National Advanced School of Engineering of the University of Yaounde I, where he is currently a senior lecturer. His area of specialization include: computer network security, cryptography and formal specification and verification; theorem proving and model checking. He has published some research articles in international journals namely *Formal model of a group key agreement protocol. Journal of Computational Technologies, 7(4):4–20, 2002*. In 2006 he was appointed Director General of the National Agency for Information and Communication Technologies Cameroon, a position he occupies till date. Major activities of the agency include amongst others: securing the Cameroon cyberspace through three key services: Computer Incidence Response Team (CIRT), Public Key Infrastructure (PKI) and Computer Security Audits.

Dr. EBOT EBOT ENAW may be reached at ebotenaw@yahoo.com