Location Identification and Alert System in Absence of GPS

Qurban A. Memon
Associate Professor, UAE University, Al-Ain, 17555, UAE
Email: qurban.memon@uaeu.ac.ae

Abstract—**There are two concerns with GPS systems. On one side, many people are becoming more aware of privacy issues that emanate from wide spread use of GPS enabled or similar systems. On the other, in absence of GPS systems emergency help is of great importance as location detection becomes not so easy. Thus, there is a need for location detection technique or a solution that not only helps in detecting location but relieves the person of the privacy concern. Such systems find widespread application in military and personal communications. In this paper, introduction to various well known systems is first presented, followed by existing location detection methods and technologies. The privacy issues are also highlighted. In order to address privacy, a location detection system is developed for a limited geographical area as a case study. The simplicity and security of data transfer are also addressed by encryption using special purpose microcontrollers. The standardization efforts for location identification are also summarized.**

Index Terms— **Location identification, Privacy in data transfer environment, Data Transfer Security, GPS vulnerability**

I. Introduction

Emergency alert and response systems are of great interest in this age of personal safety and security. Generally, there are situations in operational area like drilling, mining, defence, sub-surface or any other indoor location where global positioning devices are either in-efficient or expensive to use, and typical local/indoor or private area networking is only available option. Response to different types of emergencies in the indoor environment is critical in order to protect resources including human life. The tracking and navigation in such situations is expected to be the key to the development of user specific services and applications. In these situations, the requirement is to track the object during emergency in real time and provide rescue services dependent upon nature and priority.

A study carried out in [1] presents the current and future opportunities for portable tracking and navigation in Western Europe. In this study, it is investigated that personal navigation in Western Europe during 2007-2012 grew by about 10% annually. With the launch of iPhone and similar ones by its competitors, this market is expanding dramatically in the next few years. Similar pattern of growth is expected to be witnessed in the middle-east, especially Gulf Cooperation Council (GCC) region. There have been four fundamental market requirements to such location based services: Convenience or simplicity, Efficiency, Security, and Reliability. The fulfilling of these requirements leads to wide acceptance of such devices into the market.

For tracking personnel, vehicles or objects, there are a number of approaches suggested in literature that may be investigated to provide a solution during an operational environment. The environments include areas where GPS tracking can be deployed to provide safety and security. GPS has proliferated throughout military and civilian applications to the extent that it can be considered a "utility" similar to water, electricity, and gas. GPS receivers are known to be power-hungry [2] and an application may prefer a lower sampling rate when the mobile device's battery is low. Lower sampling frequencies result in a sparser set of track entries than otherwise. Since some applications require high precision, the Assisted GPS (A-GPS) alternative could also be too inaccurate (and too costly) for such purposes, when in a densely populated area with numerous points of interest. Current solutions thus lack in providing fool-proof privacy and are not efficient and reliable in some areas like indoors, sub-surface, etc. Additionally, the systems involving GPS have been reported to be ineffective in situations where GPS signal is affected by jammers or interferers.

Some 802.11 device drivers broadcast their existence to the infrastructure regularly. Similarly, we are not aware of any GSM cell phone on the market today that does not report itself to the infrastructure. Cell phone providers, coffee shops, and hotels probably do not mind if the existence and location of their network beacons are known. Individuals and corporations, however, may be wary in some cases of having information about their access points listed in a public database. A large number of people have, thus, become very concerned about their safety and security due to use of a variety of hi-tech devices. Though, there are significant advantages associated with their use, but the devices pose direct challenge to privacy matters of the individual or the corporate. The fear is what clever people can do with the data that is accessed or is floating around the networks. A good number of research works and projects are being executed to address these issues and the priorities, but the concerns still remain. As regards to privacy, the countless

doi:10.4304/jait.4.4.172-180

benefits of location based services (LBS) are offset by social hazards unparalleled in human history. Inherent in this concept is the potential within a central location to routinely control time, location, speed, and direction for each and every movement of the client device or, indeed, of many clients simultaneously. Furthermore, users typically visit a small set of places via predictable routes as part of their daily routine (e.g., they travel between home and school or work, they go grocery shopping, they walk the dog, etc.). These tracks expose the daily routine of the device user. Another side effect of this technology use surfaces when the navigator regularly navigates by blindly pushing buttons and reading the coordinates from "black boxes". Thus, he/she will not be prepared to use basic principles to improvise solutions in an emergency.

In a wireless environment, security may be understood by knowledge of common security standards like 802.11 WEP, 802.11 WPA and WPA2 (802.11i). One of the major flaws in WEP is its key length. WEP has a 40-bit key, which can be broken in few hours with the help of normal computer machines [3]. With new release as WEP2, its length increased from 40-bit to 104-bit key. This resolved some issues, but the disadvantage of WEP however, is the lack of key management. In addition to that, WEP does not support mutual authentication. Switching to WPA and WPA2 technologies has solved many problems on both user and company levels, but it is difficult to say that wireless networks are secure. WRAP (Wireless Robust Authenticated Protocol) is the LAN implementation of the AES encryption standard, ported to wireless to get the benefits of AES encryption.

For encryption purposes, four encryption algorithms: AES, XTEA, SKIPJACK® and an encryption algorithm using a pseudo-random binary sequence generator may be quoted, amongst many. In today's era of information technology where data is widely accessible, electronic data needs to be encrypted for user's protection. If the information is encrypted first, it has a better chance of remaining secure. Many encryption algorithms provide protection against someone reading the hidden data, as well as providing protection against tampering. In most algorithms, the decryption process will cause the entire block of information to be destroyed if there is a single bit error in the block prior to decryption.

The Data Encryption Standard (DES) algorithm adopted in 1997 [4], became a worldwide standard for data encryption by ISO (International Standards Organization) [5, 6]. The Advanced Encryption Standard (AES) is a means of encrypting and decrypting data adopted by the National Institute of Standards and Technology (NIST) on October 2, 2000. AES is a symmetric block cipher that utilizes a secret key to encrypt data. The implementation of AES, as a typical implementation is based on a 16-byte block of data and a 16-byte key size. This implementation of AES uses a 16-byte block and a 16-byte key and thus uses 10 rounds of encryption. On the last encryption round, the mix column subdivision is left out. To fit into the data matrix structure, the plain text to be encrypted needs to be broken into the appropriate size blocks, with any leftover space being padded. Finally a key must be selected that is 128-bits long. With a key selected and the data sectioned off into appropriate size blocks, the encryption cycle may now begin.

Today, the level of integration possible allows processor vendors to integrate the encryption engine into their embedded processor/microcontroller, thus making the system a bit more secure. The dedicated engine accelerates the computations so that transactions can be done in real-time with no noticeable delay, thus reducing the wait for the user and allowing the system to handle more transactions per minute. Secure MCU offerings range from 8-bit to 32-bit CPUs with dedicated encryption engines, random number generators, and additional features to secure communication channels and protected data.

II. Existing Systems and Related Work

A lot of systems concepts sail under the label of real-time locating systems. However the qualification of these approaches is very different and offers a wide variation of cost-to-benefit ratio.

A. *Locating at Choke Points*

There is class of most simple locating which applies no physical measurement at all, but just communicates at coincidence of transceiver and transponder as long as communication may happen. Then locating collapses to simple application of RFID technologies according to the equivalent standard. This is the only option to apply passive RFID tags for locating. Then the reach of the RFID reader determines the choke point. Hence accuracy is defined by the sphere spanned with the reach of the reader.

B. *Locating in Relative Coordinates*

Many references describe locating at relative coordinates. Such coordinates may be radial distances compared with reference to known locations and no angular directions. There is no exact metrics required, unless the relation to the reference points is intelligible. Such solutions may be referred as fuzzy locating.

C. *Locating in Absolute Coordinates*

The high precision of satellite navigation systems led to some snugness in setting the requirements for locating of objects. Generally the determining of absolute coordinates is the most challenging approach. A sound escape from electromagnetics and surface effects is found with ultra short pulse communications, as with ultra wide band (UWB) indoor approaches. However, many such concepts often do not serve results for the paid price when the targets move. This may be assessed by the vast number of publications and the very small references on installed solutions

D. *Locating in Contiguity*

A newer approach for locating defines a location just as the contiguous ambience of the person looking for something to be located. That is very similar to choke point locating. However, the accuracy may be much better tuned, as the reach is not influenced by the steady illumination of the tag with the reader, but just by the tuned transmission power level of an active RFID tag as an intermittent beacon. This is the easy option to apply graded active RFID tags for economized locating. Then the reach of the RFID receiver determines the base point. Hence operational suitability is defined by the algorithm for varying the minimum reach of transmission of the beacon. Solutions are available as very simple electronic leashes or in more complex designs. A very common application is with electronic wireless lock solutions. More advanced applications combine the tag operation with autonomously operating software agents, e.g. in smart phones for monitoring manually controlled systems and services.

As far as products are concerned, an approach to the problem of automatically determining the location of an individual has been to design a tag in the form of a badge [7] that emits a unique code for approximately a tenth of a second. These periodic signals are picked up by a network of sensors placed around the host building. A master station, also connected to the network, polls the sensors for badge 'sightings', processes the data, and then makes it available to clients that may display it in a useful visual form. The badge was designed in a package roughly 55x55x7mm and weighs a comfortable 40g. A disadvantage of an infrequent signal from the badge is that the location of a badge is only known, at best, to a 10-second time window. However, because in general a person tends to move relatively slowly in an office building, the information the Active Badge system provides is very accurate.

RADAR [8] is the world's first Wi-Fi signal-strength based indoor positioning system. The signal received at the mobile device is strongest when the receiver is close to the AP and weakest when further away. This trend is exploited by RADAR to estimate the mobile device's location inside a building. The RADAR system works using a radio map. A radio map is a lookup table that holds collections of packet signal strengths and the building locations where these signals were measured. To locate the user's position, the user's wireless device measures the signal strength from the APs within its range and then searches the radio map to determine the signal strength entry that best matches the measured signal strength.

The Place Lab [9] architecture consists of three key elements: Radio beacons in the environment, databases that hold information about beacons' locations, and the Place Lab clients that use this data to estimate their current location. Using Place Lab, commodity laptops, PDAs and cell phones estimate their position by listening for the cell IDs of fixed radio beacons, such as wireless access points, and referencing the beacons' positions in a cached database. Place Lab currently only generates position estimates in two dimensions (latitude and longitude) and ignores the altitude component of location. This can present a problem in multistory buildings where floor number is likely a key aspect of location.

The authors in [10] describe enhanced position location system (EPLS) serves all three services as a position location, identification, communications, and (sometimes) navigation system. The system consists of two primary components, a network control element and a network of Radio Sets (RSs). Although EPLRS can use GPS inputs when available, one of the key features of EPLRS is that it does not depend on GPS to provide position and location data, thus avoiding GPS jamming vulnerabilities.

The cricket system [11] is intended for use indoors or in urban areas where outdoor systems like the Global Positioning System (GPS) don't work well. It provides fine-grained location information---space identifiers, position coordinates, and orientation---to applications running on handhelds, laptops, and sensor nodes. Wall- and ceiling-mounted beacons placed through a building publish information on an RF channel. With each RF advertisement, the beacon transmits a concurrent ultrasonic pulse. Listeners attached to devices and mobiles listen for RF signals, and upon receipt of the first few bits, listen for the corresponding ultrasonic pulse. When this pulse arrives, the listener obtains a distance estimate for the corresponding beacon by taking advantage of the difference in propagation speeds between RF (speed of light) and ultrasound (speed of sound).

The author in [12] describes in his thesis how modern, simulation-based methods of treating signals can be used to monitor and, if necessary, to take over the GPS function on a vessel. In fact, the vessel's own radar is used to measure the distance to surrounding shores, and this data is then compared with a digital sea chart. In a submarine, information from sonar equipment is compared with a digital depth chart. In combination with data about the movement of the vessel, the correct position can be calculated. The method is based on a mathematical algorithm, a so-called particle filter, which is installed as a program in the vessel's computer system.

The StarTrack [13] is a system that enables extensive operations on tracks. A track is a discrete and sampled representation of a continuous route. Mobile devices collect tracks and opportunistically upload them to a central server. The StarTrack includes facilities for storing, comparing, clustering, indexing and retrieving tracks. It serves as the foundation for building large-scale track-based services. Each participating mobile device is assumed to have a means of determining its current location through available localization technology, such as the Global Positioning System (GPS), GSM localization, Wi-Fi hotspots, etc.

The GPS-free indoor navigation and path prediction architecture of the system proposed in [14] comprises three core components: effective localization, map representation and route planning, and plan recognition. The data flow in the system originates with the localization module receiving information from the various sensors. The raw data, from WiFi and dead reckoning, is combined using a particle filter to provide an estimate of the user's location indicating the dispersion of probability of the user's presence within an area of the building.

A LocataNet [15] positioning signal system includes a terrestrial segment (TS) and a user segment (US). There is no separate control segment. The TS includes a number of LocataLite transceivers located within or around a defined service area. The US includes any number of fixed or moving Locata user receivers (Rovers) operating within the service area and deriving locations and time within the area using signals emitted by the LocataLites in the TS. LocataNets can span areas as large as several tens of kilometers in extent, being for the most part limited by the availability of adequate line-of-sight geometries between the various elements of the LocataNet. With adequate signal power, working networks have demonstrated LocataLite-Rover operating ranges of up to 50 kilometers. LocataNets can adopt any convenient coordinate reference system, including WGS-84, or other global, regional, local, or custom grids. LocataNet's overall concept derives from the Navstar Global Positioning System (GPS). Many of its underlying elements therefore are similar to GPS. The LocataLites assume the same role as GPS satellites, and the Locata user receiver operates much like a GPS receiver. Position and time calculations for the most part use techniques similar to those of GPS.

TABLE 1:

WELL KNOWN TRACKING SYSTEMS

Sr. No.	Product/System developed	Development timeline
1	Active Badge	1992
2	Radar	2000
3	Place Lab	2003
4	EPLRS	2003
5	Cricket	2005
6	Particle Filtering Based	2005
7	RSN Program	2007
8	Star-Track	2009
9	CMU-RI-TR	2011
10	LocataNet	2011

As a summary, well known tracking systems are listed in Table 1. There is a wide variety of systems concepts and designs to provide real-time locating. A good choice is listed in [16].

Nowadays, Internet has become another source for enabling geolocation detection. As discussed above, apart from Global Positioning System (GPS), common sources of location information include location inferred from network signals such as IP address, RFID, WiFi, Bluetooth MAC addresses, and GSM/CDMA cell IDs, as well as user input. Location detection with HTML5 is pretty simple. Browsers either support navigator.geolocation or they don't. If they do, one can open up a whole world of local information to users plus log a deeper and more geographic level of statistics server side.

III. LOCATION METHODS AND TECHNOLOGIES

Locating is generally accomplished in one of the following ways

a. ID signals from nodes are identifiable to a single reader in a sensory network thus indicating the coincidence of reader and nodes.

b. ID signals from nodes are picked up by a multiplicity of readers in a sensory network and a position is estimated using one or more locating algorithms

c. Location signals from signposts with identifiers are transmitted to the moving nodes and are then relayed, usually via a second wireless channel, to a location processor.

d. Mobile nodes communicate with each other and perform metering distances.

As an example, the listener can use the time difference of arrival between the start of the RF message from a beacon and the corresponding ultrasonic pulse to infer its distance from the beacon. Every time a listener receives information from a beacon, it provides that information together with the associated distance to the attached host. The listener (or software running on the host device) infers its position coordinates based on distances from multiple beacons whose positions are known, and software running on the host device can associate itself with the space corresponding to the nearest beacon.

There are two different principles when measuring travel time of radio waves:

- Trilateration derives the travel time of a radio signal from a metering unit, and measures and computes the distance with the relation of light speed in vacuum. Another method worth mentioning is multilateration, not to be confused with trilateration. This uses distances or absolute measurements of time-of-flight from three or more sites.
- Triangulation derives the travel time of a pair of synchronous radio signals from a metering unit with two transmitters, measures and computes the difference of distance with the relation of light speed in vacuum as an angle versus the baseline of the two transmitters.

The indoor positioning could be done by several methods: Cisco Radio Frequency (RF) fingerprinting, AP triangulation or Received Signal Strength (RSS) lateration. The list includes cell of origin – the simplest way to determine the originating position (in 802.11, the associated access point), but this method could be inaccurate if mobile device is not associated to the nearest AP. For greater accuracy, this system could be combined with the Received Signal Strength Indicator (RSSI). Distance or lateration may use any of the following measurements:

- Time of Arrival (ToA) – with the emitting mobile device synchronized, ToA indicates the measured signal's traveling time, which determines the distance to the target (velocity multiplied by time); three neighboring APs create a triangulation to determine the location.
- Time Difference of Arrival (TDoA) – if the emitting mobile device is not synchronized, relative time is measured between several receiving devices that are

synchronized with each other and detect the same signal in different locations. Three neighboring APs create a hyperbolic tri-lateration.

- Angle or angulation – Angle of Arrival (AoA) is a technique that determines the angle of incidence of the received signal from the mobile station. When two APs that send signals are compared, it is possible to determine the originating location.

The information location obtained from RFID, combined with the previously described location-tracking information, opens new technological scenarios. APs transmit the information about the received signal of any WLAN client (WLAN phone, RFID tag etc.) toward the WLAN controller, and further to the Wireless Location Appliance. This application has a database that is checked against the user's reported real-time location so that the location can be shown on the browser-based console on the map of the floor plan.

As discussed before, many positioning techniques have been developed in the world. It is difficult to say, which technique provides the best solution for a specific (location-based) problem, as the number of positioning techniques is large and diverse. The choice of a specific technique is now often arbitrary. A general model for selection of the best solution for a locating problem has been constructed at Radboud University of Nijmegen [17].

IV. Location Methods and Technologies

Generally, there are situations in operational area like drilling, mining, defense, sub-surface or any other indoor location where global positioning devices are either in-efficient or expensive to use, and typical local/indoor or private area networking is only available option. The tracking and navigation in such situations is the key to the development of user specific services and applications. Each track is a sequence of entries recording a person's time, location, and application-specific data. A track is intended to capture the path taken by a mobile device or, more importantly, a person in possession of a mobile tracking device. Each track entry is a tuple consisting of a location, time, and optional application specific metadata in the form of an XML document with arbitrary contents. As an example, Star Track [18] provides applications with a comprehensive set of operations for recording, comparing, clustering and querying tracks. The key consideration with this collection of tracks is its misuse.

Users typically visit a small set of places via predictable routes as part of their daily routine (e.g., they travel between home and school or work, they go grocery shopping, they walk the dog, etc.). Through track clustering, the system allows applications to eliminate near duplicate tracks and group tracks into a smaller set of representative tracks. However, as discussed before, GPS receivers are power-hungry [2] and when the mobile device's battery is low, an application may prefer a lower sampling rate. Lower sampling frequencies result in a sparser set of track entries than otherwise. Differences in the speed of motion (e.g., walking at 3 mph or cycling at 15 mph or driving at 40 mph) also cause variations in the track entries. Furthermore, terrain (e.g., a steep hill) or traffic congestion can also cause noticeable speed variation. Thus even with a fixed sampling frequency, one can end up with dissimilar track entries for a path.

In these systems, privacy problems arise from four sources: Content, Location, Tracks, and Metadata. Privacy threats do not only arise from the tags and locations provided, but also from tracks that a mobile tagging application can record. As a summary, it may be safely said that respective solutions to date are not mature enough to address the tracking during emergency duration only, and maintain privacy at the same time.

V. Implementation – A Case Study

In this work, an effort is made to provide location detection in order to enable rapid emergency response, by developing a system that supplements wireless communications distributed throughout the user operational area. The users are expected to be issued a device that will attach a key chain, for example, as a transmitter. The pressing of the button enables transmission of user (ID) data. The signal propagates throughout the network, and reaches receiver where location of the user is calculated. It is assumed that location detection is calculated in absence of GPS systems. The receiver application runs on a computer. The objective set in this work is privacy, safety and security to be felt by employees at work in return for willingness and productivity of the employee.

Three options were investigated to develop user device. First, Pocket PC was considered for an application development to be used by a user to send a signal to wireless access points/receivers once it is operated. Since, it is highly likely that Pocket PC would be ON all the time hence location information is always available (like GPS system). This creates privacy concerns. The second option investigated was use of a Wireless USB (WUSB) device connected to a Microcontroller Unit (MCU) and with a button to control it for sending a signal. In this option, it turned out that it may not be easy or preferable to interface WUSB to MCU. This raised a customization issue, as commercial WUSB's come with set constraints. Third option investigated was use of RF devices. In this case, the chip coverage may be extended if desired. But it requires a whole new system to be built up from scratch, and the concern that it would not be compatible with IEEE 802.11 standard based systems.

Any of the previous options has its own difficulties. The choice opted was a user device simpler than WUSB but compatible with IEEE 802.11 standards as these are widely deployed nowadays. The receiver application has a Visual Basic interface that receives user signal and displays calculated user coordinates onto a map.

A. Location Calculation Method

Two methods were investigated to calculate the location of the user. One method was triangulation method and the other was GPS based position method. The related equations to be used for location calculation are shown below

$$d_1 = c(t_{t,1} - t_{r,1} + t_c) = \sqrt{(x_1 - x)^2 + (y_1 - y)^2 + \sqrt{(z_1 - z)^2}}$$
$$d_2 = c(t_{t,2} - t_{r,2} + t_c) = \sqrt{(x_2 - x)^2 + (y_2 - y)^2 + \sqrt{(z_2 - z)^2}}$$
$$d_3 = c(t_{t,3} - t_{r,3} + t_c) = \sqrt{(x_3 - x)^2 + (y_3 - y)^2 + \sqrt{(z_3 - z)^2}}$$
$$d_4 = c(t_{t,4} - t_{r,4} + t_c) = \sqrt{(x_4 - x)^2 + (y_4 - y)^2 + \sqrt{(z_4 - z)^2}}$$

The following Figure 1 shows how these equations will be used to estimate location. Each equation represents an access point that receives a signal. Each access point should have the same receiver and transmitter target. It was determined that in order to find the location of the users, at least three access points should receive the signal or (four to get accurate location). The push button is represented by the push button of the user and the receiver side is represented by the access points.

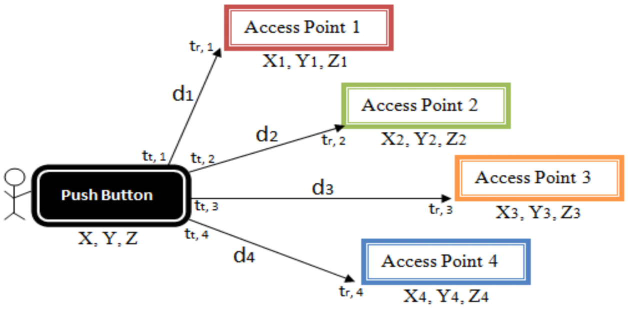


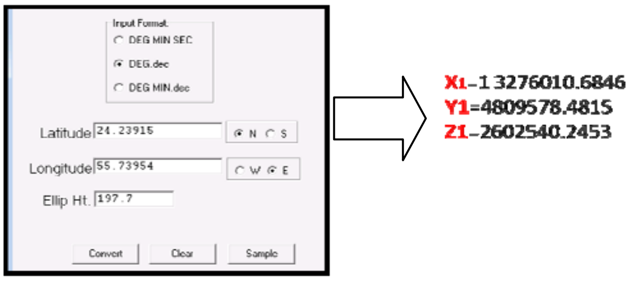
Figure 1: Location estimation

For the transmitter, there are three unknowns X, Y, Z. The X, Y, Z parameters represent the coordinates of user (push button), which are to be calculated after all variables are substituted in equation (1). There is a fourth unknown 'time correction (t_c)' – access point receiver clock - which is to be calculated after all variables are substituted in the equation (1). Thus, the requirement is to find four unknowns (X, Y, Z, tc). The variable 'c' in the equations represents the speed of signal that propagates through access points. The variables (X_1, Y_1, Z_1) represent coordinates of access point 1, (X_2, Y_2, Z_2) represent coordinates of access point 2, etc. So, for the receiver to calculate user location, the coordinates of all access points should be known.

B. *Access Points Coordinates*

In order to measure all access points' coordinates, commonly available GPS method was used and verified by Google earth software program to determine coordinates. It turned out that measuring the access point coordinates by GPS device is not that easy as GPS devices require open area to measure coordinates as opposed to access points that are inside the building. Thus, Google earth software was used to get readings in degree and decimal format for coordinates of all access points. The readings consisted of three points, which are:

i Longitude
ii Latitude
iii Height


Input Format
○ DEG MIN SEC
● DEG.dec
○ DEG MIN.dec
Latitude 24.23915 ● N ○ S
Longitude 55.73954 ○ W ● E
Ellip Ht. 197.7

X1–1 3276010.6846
Y1=4809578.4815
Z1–2602540.2453

Figure 2: Coordinate Conversion

The equations need only X, Y, Z format for access point coordinates in order to do calculation and find user location. A conversion program, as shown in Figure 2 was used to convert degree and decimal format to X, Y, Z format. The IP address of the user device, transmit time and receive time of data packet are recorded in the receiver, whereas IP address of each access point is stored in receiver application. A code written in Matlab solves the multiple non-linear equations to calculate the location of a person. Solving these non-linear equations gives the exact location X, Y, Z of the sender. In order to solve the four equations "ifsolve" function in Matlab was used. After an initial value is inserted for each unknown, then "ifsolve" function iterates till it reaches the correct value of each unknown.

To simulate this setup, the following devices were used: Microchip Explorer 16 board along with Wi-Fi PICtail, MPLAB ICD3, MPLAB IDE, PC, and Linksys Wireless-G router as access point. Additionally, an interface program was developed between Visual Basic (VB) and Matlab in order to pass parameters between them. A Visual Basic code was also written to convert real x, y values to VB x, y values. An overall view of graphical user interface for two area maps is shown in Figure 3. In Figure 3, '1', '2', '3', '4', '5', '6', '7', and '8' represent map view, x-y coordinates, map selection, MAC address of access points, transmission and reception time, run application, showing results, and database respectively.

C. *Determining the Location of the User Device*

If only one access point received the signal from the holder of the device, then the location of the holder of the device will be within the range of the access point itself. But, if more than one access point received the signal, then the location of the holder of the device may be the intersection of these access points range. So, as more access points receive the signal, the more accurate and precise location of the user can be defined by the system equations, as depicted in Figure 3. To make application run faster, it was determined that the Matlab code and database may be translated to VB so that the application uses only one tool to do all tasks in the receiver.

From the study of availability of similar and compatible projects, it was found out that such technologies were being used either for medical purposes or for tracking purposes (using GPS devices). There are commercial companies available, which offer this service to senior citizens or to people who need a continuous monitoring due to some health issues, so the company provides them a 24 hour monitoring by letting the user have a small device such as a watch or a key chain to send a signal to another device plugged into a telephone line. One of the main issues with such designs is the concern for privacy. In our implementation, location signal would be available in the air, when user push-button is pressed.

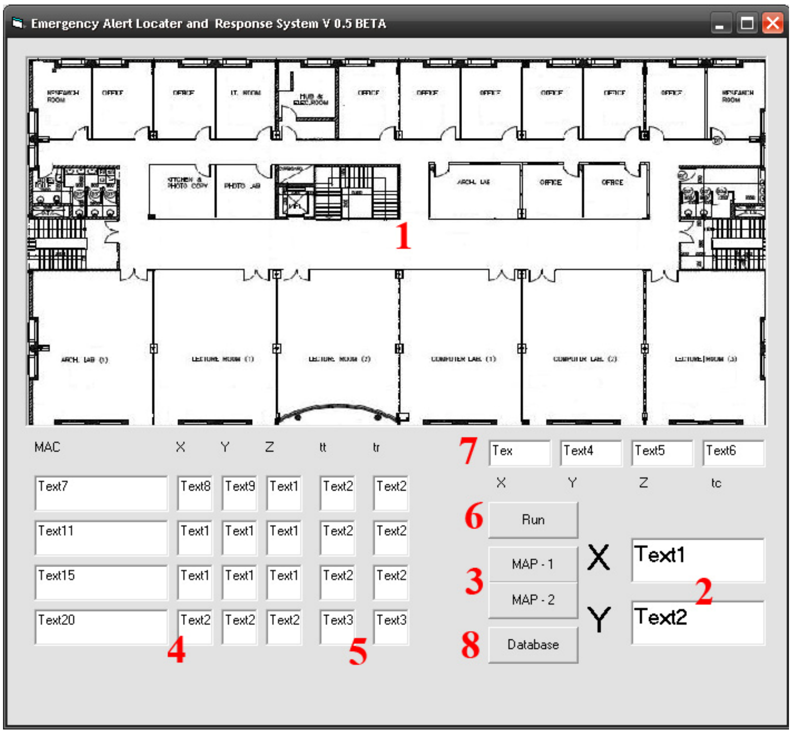


Figure 3: A sample view of graphical user interface

D. *Protecting Data over WLAN*

Though pressed-key data once in the air enables calculation of the location, but this transmission of pressed-key data may be sent through secured noise-free channels, as discussed in [19, 20], or the data privacy can further be enhanced by the use of encryption techniques. This encryption process will only start when the user presses the key. Many embedded processor vendors — Atmel, Freescale, Maxim, Microchip, NXP, PalmChip, STMicroelectronics, Texas Instruments, and others — have included dedicated encryption/decryption engines and random number generators on their processor chips. Additionally, encryption engine blocks are available from several vendors of intellectual property, and such blocks can be co-integrated with a processor core on a custom chip, or embedded in a field programmable gate array along with a processor core.

Based on its proprietary 8-bit PIC processor core, Microchip offers security-enhanced processors, such as the PIC12F635/PIC16F636/639. These 8-bit processors include a cryptographic module the company calls KEELOQ. The module employs a block-cipher encryption algorithm based on a block length of 32 bits and a key length of 64 bits. The algorithm obscures the information in such a way that even if the unencrypted/challenge information differs by only one bit from the information in the previous challenge; the next coded response will be totally different. Statistically, if only one bit in the 32-bit string of information changes, approximately 50 percent of the coded transmission will change. A bit rate of about 51 Kbps baud can be achieved, with a device utilization of 100%. This makes the PIC17C42 a price/performance leader for encryption algorithms.

Based on this investigation, it was decided to embed encryption of pressed-key data (within PIC microcontroller) to be transmitted from the user device. The objective was to encrypt the identification of the device that pressed the key. As data size is small, necessary padding was done to create 16-byte data blocks. For implementation purposes, the key “This is my data ” was used. Once key was selected and data partitioned, the encryption cycle was started. For this purpose, the specific Advanced Encryption System (AES) encryption libraries and routines [21] were used for Microchip microcontroller. When the data is received at the receiver, the respective decryption process is started. This process is carried out in a similar microcontroller, as a part of receiver. The subdivisions of the decryption algorithm are similar to those of the encryption algorithm, with most being the inverse operation. The decryption key is different than the encryption key and must be loaded correctly. If, during encryption process, the key is not reset between blocks, the decryption key will then have to adjust accordingly. Each round of AES decryption uses the same key that was used to encrypt the data. The key for the next iteration can be determined from the previous decryption key by performing the inverse operation to the encryption key schedule. To obtain the decryption key from the encryption key, cycle the appropriate amount of times through the encryption key schedule. At the end of an encryption cycle, the value of the key at that point is the correct decryption key, so this value can be saved, recalculated later or pre-calculated and stored in the system. As the microcontroller completes the decryption in real time, the location calculation is started.

If absolute security is needed no matter what the speed, cost or code size, then the best choices are XTEA technique with 32 or more rounds or AES . A balance between code size, execution speed and security is XTEA with 16 iterations. When developing a system that needs to securely talk to other systems, it will be necessary to implement the same encryption standard so the communication can be deciphered.

VI. Standardization

The standards do not stipulate any special method of computing locations, or the method of measuring locations. This may be defined in specifications for triangulation or any hybrid approaches to trigonometric computing for planar or spherical models of a terrestrial area. The basic issues of RTLS are standardized by the International Organization for Standardization and the International Electrotechnical Commission, under the ISO/IEC 24730 series. In this series of standards, the basic standard ISO/IEC 24730-1 identifies the terms describing a form of RTLS used by a set of vendors, but does not encompass the full scope of RTLS technology.

Currently several standards are published or under discussion:

- ISO/IEC FDIS 19762-5 Information technology AIDC techniques — Harmonized vocabulary, Part 5 — Locating systems
- ISO/IEC 24730-1:2006 Information technology real-time locating systems (RTLS) Part 1: Application program interface (published).
- ISO/IEC 24730-2:2006 Information technology real-time locating systems (RTLS) Part 2: 2,4 GHz Air interface protocol (published, WhereNet/Zebra approach).
- ISO/IEC WD 24730-5 Information technology real-time locating systems (RTLS) Part 5: (drafted ISO/IEC standard out for balloting in 2008, Nanotron approach).
- ANS/INCITS 371 series: Information Technology – Real-Time Locating Systems (RTLS). The Committee approved three new standards in 2003 that define two Air Interface Protocols and a single Application Programming Interface (API) for Real Time Locating Systems (RTLS), especially for use in asset management.

A lot of work for location detection standardization in domain of 3G mobile phone systems has been carried. A summary of standardization for 3G, 3GPP, and 3GPP2 enabled mobile systems is provided in [22].

VII. Conclusions

A real time locating system was developed to determine location positioning during emergency duration to secure privacy at all times. This was enabled in the system by a push button and encryption. The accuracy of location detection is however, dependent on the method used to calculate it. If only one access point receives the signal from push button device, then the location range is the coverage area of one access point only. In case two access points receive the signal, then the accuracy is within intersection of these access points' range. Thus, if more access points receive the signal, better accuracy is ensured. In conclusion, the implemented system boosts privacy by a) no data transfer except during emergencies b) encrypting data during emergency. Such a deployed system facilitates the safety management departments to address personal safety and security of the user in an operational area.

Acknowledgment

This work is supported by Research Affairs unit of College of Engineering, United Arab Emirates University, Al-Ain under Grant Code. G00000814, 2011-2012.

References

[1] Gibson, B., Cory, T., "Portable Navigation and Wireless Tracking: Western Eurpoean Markets and Forecasts 2007-2012", Juniper Research: www.juniperresearch.com; accessed on November 11, 2010.

[2] Mohan, P. et al. Nericell: Rich Monitoring of Road and Traffic Conditions using Mobile Smartphones, Proceedings of the 6th ACM Conference on Embedded Networked Sensor Systems, US, 2008, doi: 10.1145/1460412.1460444.

[3] Brown, B.,"802.11: the security differences between b and I", IEEE Potentials, Volume 22, Issue 4, Oct-Nov 2003, Page(s):23–27.

[4] NBS FIPS PUB 46, "Data Encryption Standard," National Bureau of Standards, US Department of Commerce, January 1977.

[5] SO DIS 8730, "Banking Requirements for Message Authentication (Wholesale)," Association for Payment Clearing Services, London, July 1987.

[6] ISO DIS 8732, "Banking Key Management (Wholesale)," Association for Payment Clearing Services, London, December 1987.

[7] Hopper, A., Harter, A., Blackie, T., "The Active Badge System", INTERCHI'93, Amsterdam, April 1993.

[8] http://research.microsoft.com/en-us/projects/radar/, accessed online April 2012.

[9] LaMarca, et. al., "Place Lab: Device Positioning System using Radio Beacons in the Wild", Intel Research, IRS-TR-04-016, October, 2004.

[10] Tharp, D., Wallace, L., "Enhanced Position Location Reporting System: Legacy System Provides New Technology for Warfighters", Navigation and Applied Sciences, SSC San Diego Biennial Review, 2003, pp. 206-211.

[11] Nissanka B. Priyantha, Anit Chakraborty, Hari Balakrishnan, The Cricket Location-Support system, Proc. 6th ACM MOBICOM, Boston, MA, August 2000.

[12] Karlsson, R., “Particle Filtering for Positioning and Tracking Applications”, PhD Thesis, Linkoping University, SE-581-83, Sweden, Linkoping 2005.

[13] Ananthanarayanan, G., et al, “StarTrack: A Framework for Enabling Track-Based Applications”, Microsoft Research, 2011.

[14] Meneguzzi, F., et al, “Predictive Indoor Navigation using Commercial Smart-phones”, IEEE Percom.

[15] LocataNet Positioning Signal Interface Control Document-2011, Locata Corporation, Ltd, 111 Canberra Avenue, GRIFFITH ACT 2607, Australia.

[16] Malik, A., RTLS For Dummies, Wiley, April 2009

[17] Koppers, J., Positioning Techniques: A general model: http://www.positioningtechniques.eu/, Accessed on June 5, 2012.

[18] Ananthanarayanan , G., Haridasan, M., Mohomed, I., Terry, D., Thekkath, C., “StarTrack: a framework for enabling track-based applications”, Proceedings of the 7th International Conference on Mobile systems, Applications, and Services, June 22-25, 2009, Kraków, Poland.

[19] T. Kasparis, M. Georgiopoulos, Q. Memon, “Direct-sequence Spread-Spectrum with Transform Domain Interference Suppression”, *Journal of Circuits, Systems, and Computers*, Vol. 5, Issue, 2, 1995, pp. 167-179.

[20] Q. Memon, T Kasparis, “Transform coding of signals using approximate trigonometric expansions”, *Journal of Electronic Imaging*, 6 (04), pp. 494-503

[21] Flowers, D., “Data Encryption Routines for PIC18 Microcontrollers”, 2011, http://www.microchip.com/stellent/idcplg?IdcService=SS_GET_PAGE&nodeId=1824&appnote=en022056, last accessed October 4, 2012.

[22] Zhao,Y., “Standardization of Mobile Phone Positioning for 3G Systems”, IEEE Communications Magazine, pp. 108-116, July 2002..

Qurban A Memon has contributed at levels of teaching, research, and community service in the area of electrical and computer engineering. He has authored/co-authored over eighty publications in his academic career. He has executed research grants and development projects in the area of microcontroller based systems; and networks. He has served as a reviewer of many international journals and conferences; as well as session chair at various conferences. His research interests include intelligent systems and networks.