*International Journal of Scientific and Innovative Research 2017; 5(2) : 83 - 90*
*P-ISSN 2347-2189, E- ISSN 2347-4971*

# SECURITY FOR DEVELOPMENT OF GPS EDUCATIONAL SYSTEM

***Madhulata Nirmal**

Department of Computer Science, Naraina College of Engineering &Technology, Kanpur, Uttar Pradesh, India

*Address for correspondence: Dr. Madhulata Nirmal, Associate Professor, Department of Computer Science, Naraina College of Engineering &Technology, Kanpur,Uttar Pradesh, India ;
**E mail ID** : madhusgi@gmail.com

## ABSTRACT

*Now days, the whole word feels insecure; the environment knows no peace and the people can't sleep with even one of their eyes closed. These are apparently evidenced in incessant wars between nations that have resulted in genocide and carnage while extent of damages, "Crimes against Humanity"being perpetrated by man against fellow man who has wrecked on lives and properties cannot be quantified. The sounds of guns, Weapons of Mass Destruction (WMD) and Bomb blasts have enveloped the entire world. This paper explores how to secure the GPS educational system using crypto concept by which the secure education can extended in the whole world for human developments.*

***Keywords:*** *GPS; Educational System; Kit;*

## INTRODUCTION

The well-known Global Positioning System (GPS) is a satellite-based location system made up of a network of 24 satellites placed into orbit by the U.S. Department of Defense. In these days, GPS has various applications on land, at sea and in the air. Basically, GPS is usable everywhere except where it is impossible to receive the signal such as inside most buildings, in caves and other subterranean locations, and underwater.[1-3] The most famous application is vehicle navigation system with which many cars are equipped. Many knows GPS by name, however, they often does not know the principle of it. Therefore it is necessary to develop an educational system to educate basic principles of GPS. In this paper, an educational system is developed to educate basic principles of GPS. The system is composed of a kit and a monitoring program. The kit is composed of a GPS antenna and a board which contains a GPS receiver. It receives GPS signal through the antenna and transmit to computer through serial cable. The program, developed with MFC using Visual Studio v.6.0[4], has many functions such as (1) receiving and displaying GPS signal from the kit, (2) reading and displaying a logged data from a file, (3) displaying current position of satellites in view, (4) displaying SNR of each satellite in view by bar graph, (5) showing current user 3-D position, (6) interfacing with ALMAP and creating map showing current user position from ALMAP, and (7) eventually enabling a user to construct his own navigation system.

User can be learned through the system:
Positioning principle of GPS.
NMEA format.
Principle of map display.
Characteristics of GPS signal such as signal to noise ratio and Dilution of Precision (DOP).

## GLOBAL POSITIONING SYSTEM

The Global Positioning System was developed to highly accurate position, velocity, and time information to an unlimited number of properly equipped users anywhere on the ground, at sea, in the air, out in space. As a universal positioning system, GPS provides several characteristics not found in other existing equipment which will enhance the conduct of mission operations.[5] These include (1) extremely accurate three-dimensional 3-D position, velocity, and time (2)

The well-known Global Positioning System (GPS) is a satellite-based location system made up of a network of 24 satellites placed into orbit by the U.S. Department of Defense. In these days, GPS has various applications on land, at sea and in the air. Basically, GPS is usable everywhere except where it is impossible to receive the signal such as inside most buildings, in caves and other subterranean locations, and underwater.[1-3] The most famous application is vehicle navigation system with which many cars are equipped. Many knows GPS by name, however, they often does not know the principle of it. Therefore it is necessary to develop an educational system to educate basic principles of GPS. In this paper, an educational system is developed to educate basic principles of GPS. The system is composed of a kit and a monitoring program. The kit is composed of a GPS antenna and a board which contains a GPS receiver. It receives GPS signal through the antenna and transmit to computer through serial cable. The program, developed with MFC using Visual Studio v.6.0[4], has many functions such as (1) receiving and displaying GPS signal from the kit, (2) reading and displaying a logged data from a file, (3) displaying current position of satellites in view, (4) displaying SNR of each satellite in view by bar graph, (5) showing current user 3-D position, (6) interfacing with ALMAP and creating map showing current user position from ALMAP, and (7) eventually enabling a user to construct his own navigation system.

User can be learned through the system:

Positioning principle of GPS.

NMEA format.

Principle of map display.

Characteristics of GPS signal such as signal to noise ratio and Dilution of Precision (DOP).

## GLOBAL POSITIONING SYSTEM

The Global Positioning System was developed to highly accurate position, velocity, and time information to an unlimited number of properly equipped users anywhere on the ground, at sea, in the air, out in space. As a universal positioning system, GPS provides several characteristics not found in other existing equipment which will enhance the conduct of mission operations.[5] These include (1) extremely accurate three-dimensional 3-D position, velocity, and time (2) A worldwide common grid easily converted to other local datum's (3) Passive, all-weather operation (4) Real-time and continuous information (5) Survivable in a hostile environment.

GPS is a spaced-based radio-positioning and time-transfer system. It comprises three major segments: Space, Control, and User.

The Space Segment, when fully operational, will have an Earth-orbiting constellation of 24 satellites in six planes. They will operate in nominally circular 20,200 kilometer altitude orbits inclined at an angle of 55 degrees with a 12-hour period. The spacing of satellites in their orbital planes will be arranged such that a minimum of four satellites will be in view everywhere on or near the surface of the Earth at any time. Each satellite is designed to broadcast a pair of L-band radio frequency signals, known as Link1 (L1) and Link2 (L2).

The L1 signal carries a precision ranging code and a course/acquisition ranging code, while L2 carries only precision ranging code. Super-imposed on these codes are low-rate navigation message data, including satellite clock and ephemeris parameters, satellite signal health data, and Coordinated Universal Time (UTC) synchronization information.

The Control Segment includes a Master Control Station along with a number of Monitor Stations and Ground Antennas located around the world. The Monitor Stations use a specialized GPS receiver to passively track all satellites in view. The information from Monitor Stations is processed at the Master Control Station to determine navigation message of each satellite. This updated information is transmitted to the satellites via the Ground Antennas.

The User Segment consists of a variety of User Equipment sets, associated support equipment, and other items. The User Equipment sets, passively operating on the L-band RF signals received from the orbiting satellite constellation, can provide position, velocity, and time data to appropriately equipped users with pre-designed accuracies. The GPS User Equipment sets can be integrated with other self-contained navigation systems to provide accurate positioning under the adverse operating and environmental conditions.

## DEVELOPMENT GPS EDUCATIONAL KIT

The details of the developed GPS educational kit are given below. As shown in Figure 1, the developed educational system consists of GPS kit developed, GPS receiver, AC adapter, USB cable for a power source from computer, and a computer installed MFC development tool (Visual Studio). GPS antenna is connected to the GPS kit and the GPS kit communicates with the computer through a serial port. The AC adapter and/or USB cable are used to supply power to the GPS kit. The USB cable can be used to supply power to the GPS kit from computer if there is no AC power available.

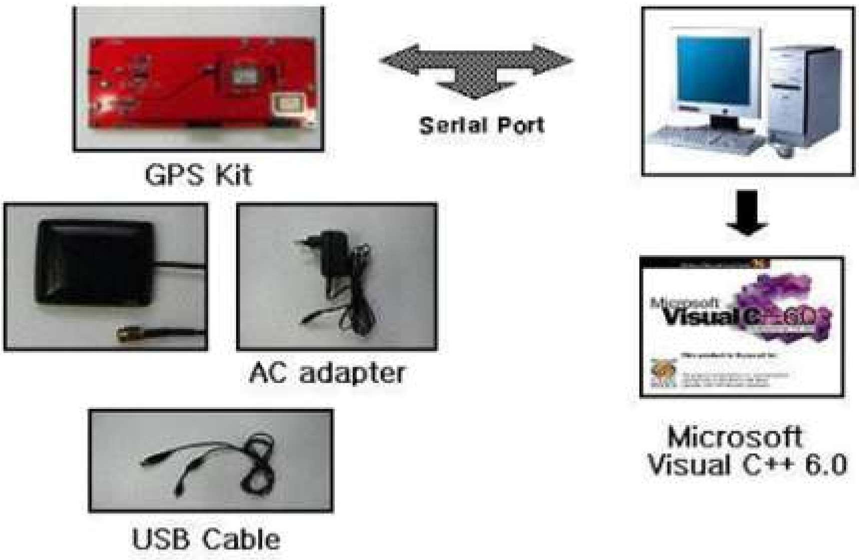


Figure 1 : Composition of the developed GPS educational kit

## DEVELOPMENT OF EDUCATIONAL SOFTWARE

A monitoring program is developed to communicate with the GPS kit to educate basic GPS principles. The developed software has various functions as follows.

- Display satellites in view.
- Display signal to noise (S/N) ratio for each satellite
- Real-time positioning
- Navigation with variable speed using pre-logged data from a file
- Show useful data such as latitude, longitude, altitude, PDOP, HDOP, VDOP and UTC
- Show the received data in NMEA format
- Use commercial map for navigation

### Security Lemma

Cryptography is widely used in networks. It can be applied anywhere in GPS stack, though it is not common at physical level. The level at which cryptography is applied directly affects its transparency to the user, and its purpose. Cryptography, as we will see, is used for much more data than data confidentially. Indeed, none of the above mentioned security services would be possible to offer without cryptography. As mentioned previously, these services rely on a combination of various security mechanisms, most of which rely on cryptography in one or another. Cryptography is also used in complicated protocols that help to achieve different security services, thus called security protocols. These protocols also rely on various cryptographically based mechanisms to achieve the desired result.

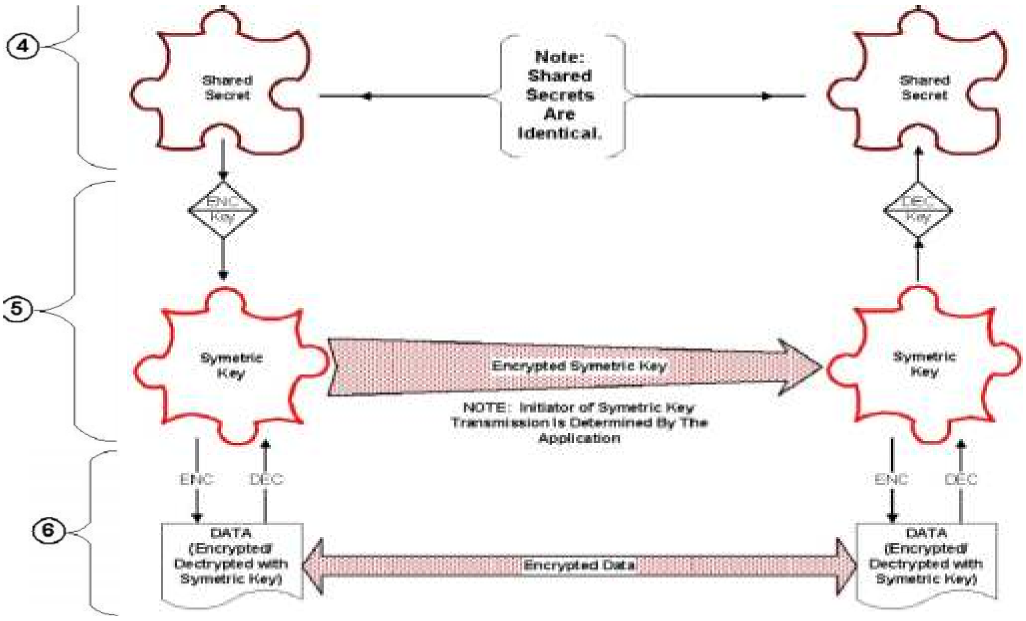

4
Shared Secret
Note: Shared Secrets Are Identical.
Shared Secret
ENC Key
DEC Key
5
Symetric Key
Encrypted Symetric Key
Symetric Key
NOTE: Initiator of Symetric Key Transmission Is Determined By The Application
ENC
DEC
ENC
DEC
6
DATA (Encrypted/ Decrypted with Symetric Key)
Encrypted Data
DATA (Encrypted/ Decrypted with Symetric Key)

Figure2: Search Network using Authentic Key

**Network using Authentic Key**

Let A and B's identities IDA and IDB are interpreted as a "contract" to use security only for this session instance and only between A and B. Public key versions of key establishment based on signatures and asymmetric encryption also exist, but we will close with one last public key variant based on a completely different asymmetric key principle called the Hellman algorithm. The Hellman algorithm is based on the discrete logarithm problem in finite groups. A group G is a mathematical object that is closed under an associative multiplication and has inverses for each element in G. The prototypical example of a finite group is the integers under addition modulo a prime number p. The idea is to begin with an element g of a finite group G that has a long period. This means to g111 * g, g2 11 * g and g311 g. Since G is finite, this sequence must eventually repeat. It turns out that g11 gn for some integer n > 1, and gn11e is the group's neutral element. The element e has the property that h< e < h 11 for every element h in G, and n is called the period of g. With such an element it is easy to compute powers of g, but it is hard to compute the logarithm of gk. If g is chosen carefully, no polynomial time algorithm is known that can compute k from gk. This property leads to a very elegant key agreement scheme:

ka = ya mod p .........................(1)

Where k is the generated key for all session G and p is prime for random search of networks. We can generate other key for b as equation (1)

kb = xb mod p.........................(2)

If x and y are two public exchange than for output session key

x = ga mod p.........................(3)

y = gb mod p.........................(4)

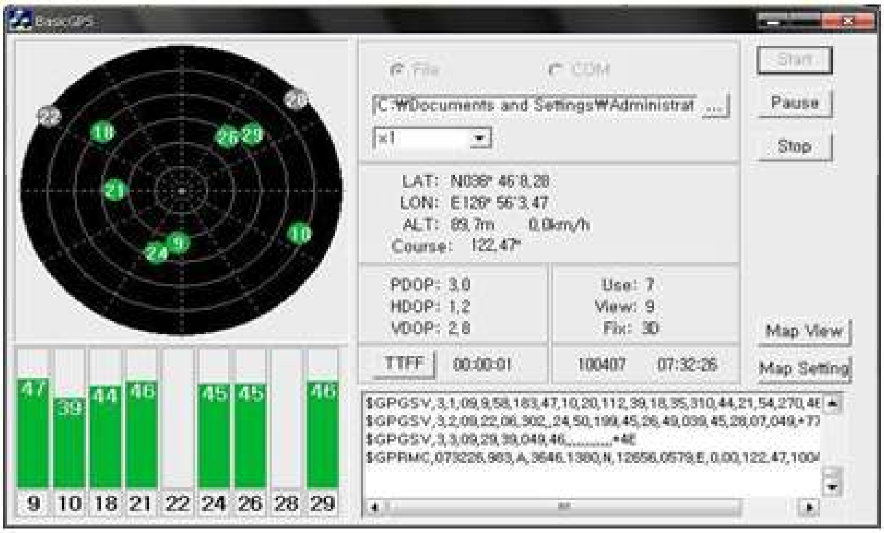
The session key is then computed as (K, ga gb). In this protocol, a is a random number chosen by A, b is a random number chosen by B, and 0 denotes the all zeros key. Note that A sends ga unprotected across the channel to B. The quantity gab is called the Diffie-Hellman key. Since B knows the random secret b, it can compute (gab)V (ga)b from A's public value ga, and similarly A can compute gab from B's public value gb. This construction poses no risk, because the discrete logarithm problem is intractable, so it is computationally infeasible for an attacker to determine a from ga. Similarly, B may send gb across the channel in the clear, because a third party cannot extract b from gb. B's signature on message 2 prevents forgeries and assures that the response is from B. Since no method is known to compute gab from ga and gb, only A and B will know the Diffie-Hellman key at the end of the protocol. The step K and gab extract all the computational entropy from the Diffie-Hellman key.

The construction (K, ga gb, ) computes a session key, which can be split into encryption and message authentication keys as before.

```
Service
{
Port     = XXXX Socket_type = stream Protocol
= tcp
Wait     = no
User     = root Passenv            = PATH
Server = /usr/local/bin/cvs
Server_args = -f --allow-root=/usr/cvsroot
pserver
}
```

Main Window

Fig. 2 shows the main window of the developed monitor program. The left-top part of the fig.2 is shown the satellites in view. The green circles denote satellites used to calculate user position and the grey circles denote satellites just tracked. The number in the circle means ID for each satellite. The left bottom part of the fig. 2 shows signal to noise ratio for each satellite, which transmitted from each satellite. The numbers under the bars are the ID number of the satellites, too. The number in the upper side of the bars denotes the signal to noise of the satellites, respectively.



C:₩Documents and Settings₩Administrat ...
x1

LAT: N036° 46'8.28
LON: E126° 56'3.47
ALT: 89.7m 0.0km/h
Course: 122.47°

PDOP: 3.0
HDOP: 1.2
VDOP: 2.8

Use: 7
View: 9
Fix: 3D

TTFF 00:00:01

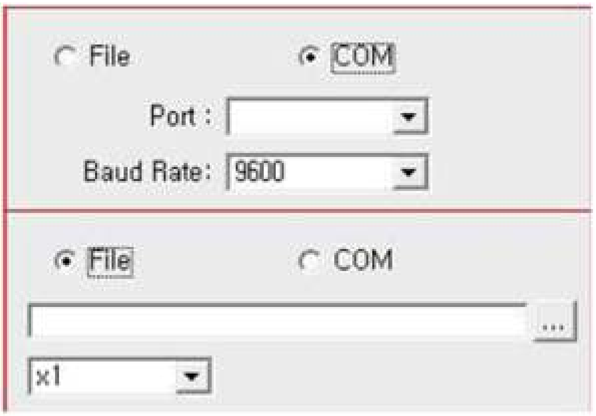
100407 07:32:26

```
$GPGSV,3,1,09,9,58,183,47,10,20,112,39,18,35,310,44,21,54,270,4E
$GPGSV,3,2,09,22,06,302,,24,50,199,45,26,49,039,45,28,07,049,*77
$GPGSV,3,3,09,29,39,049,46,,,,,,,,,*4E
$GPRMC,073226.983,A,3646.1380,N,12656.0579,E,0.00,122.47,100
```

Figure 3 : The developed monitor program

The radio buttons, 'File' and 'COM', can be selected to choose mode. Fig. 3 shows each case. If 'File' button is clicked, the system is operating with pre-logged data from a file. A file can be selected if the button captioned '.' is clicked. Various replay speed can be selected through the list box.

If the 'COM' button is clicked, we can select appropriate serial port and baud rate to communicate with the GPS kit. In this mode, the system provides real-time positioning. The received data are logged into a file like figure 4.



○ File ● COM

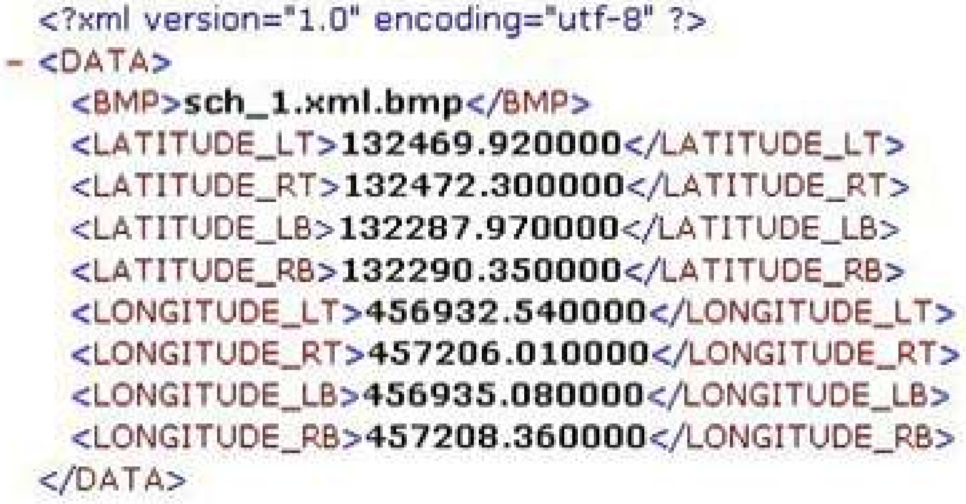
Port :

Baud Rate: 9600

● File ○ COM

x1

Figure 4: Operation mode



```
  <?xml version="1.0" encoding="utf-8" ?>
- <DATA>
    <BMP>sch_1.xml.bmp</BMP>
    <LATITUDE_LT>132469.920000</LATITUDE_LT>
    <LATITUDE_RT>132472.300000</LATITUDE_RT>
    <LATITUDE_LB>132287.970000</LATITUDE_LB>
    <LATITUDE_RB>132290.350000</LATITUDE_RB>
    <LONGITUDE_LT>456932.540000</LONGITUDE_LT>
    <LONGITUDE_RT>457206.010000</LONGITUDE_RT>
    <LONGITUDE_LB>456935.080000</LONGITUDE_LB>
    <LONGITUDE_RB>457208.360000</LONGITUDE_RB>
  </DATA>
```

**Map Setting Window**

One of the outstanding features of the system is that it is independent of special map. It can use any commercial map. It has been a big program to get a map for GPS educational system because digital map is very expensive and format is often confidential. But a technique to use a cheap commercial map is devised in this paper.

Figure 5 shows map setting window of the system. The figure shows how the technique is working. First, execute the commercial map like back most map in figure. 5. If we click the 'Map Setting' button in the Main Window, the Map Setting Window is shown. Click the left button of the mouse on the Map Setting Window and drag on the commercial map to be selected. If the red box is shown like the figure, then release the mouse left button. If we click 'Setting' button for each edge, the longitude and latitude coordinate of the selected map is appeared at the bottom of the Map Setting Window. Type the longitude and latitude coordinate of four edges of the selected map and click the 'Click' button, and the shown map is saved for later use and the saved map automatically displayed if user position is into the boundary of the map.

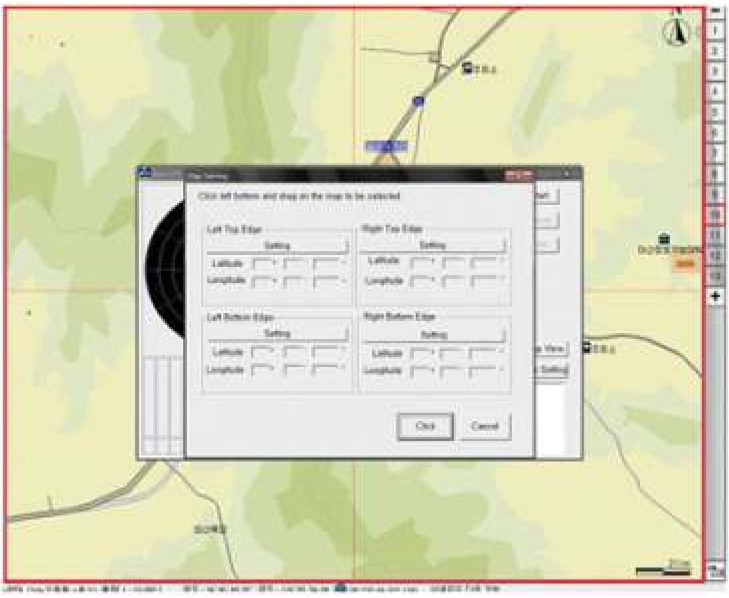


Figure 5 : Map Setting Window

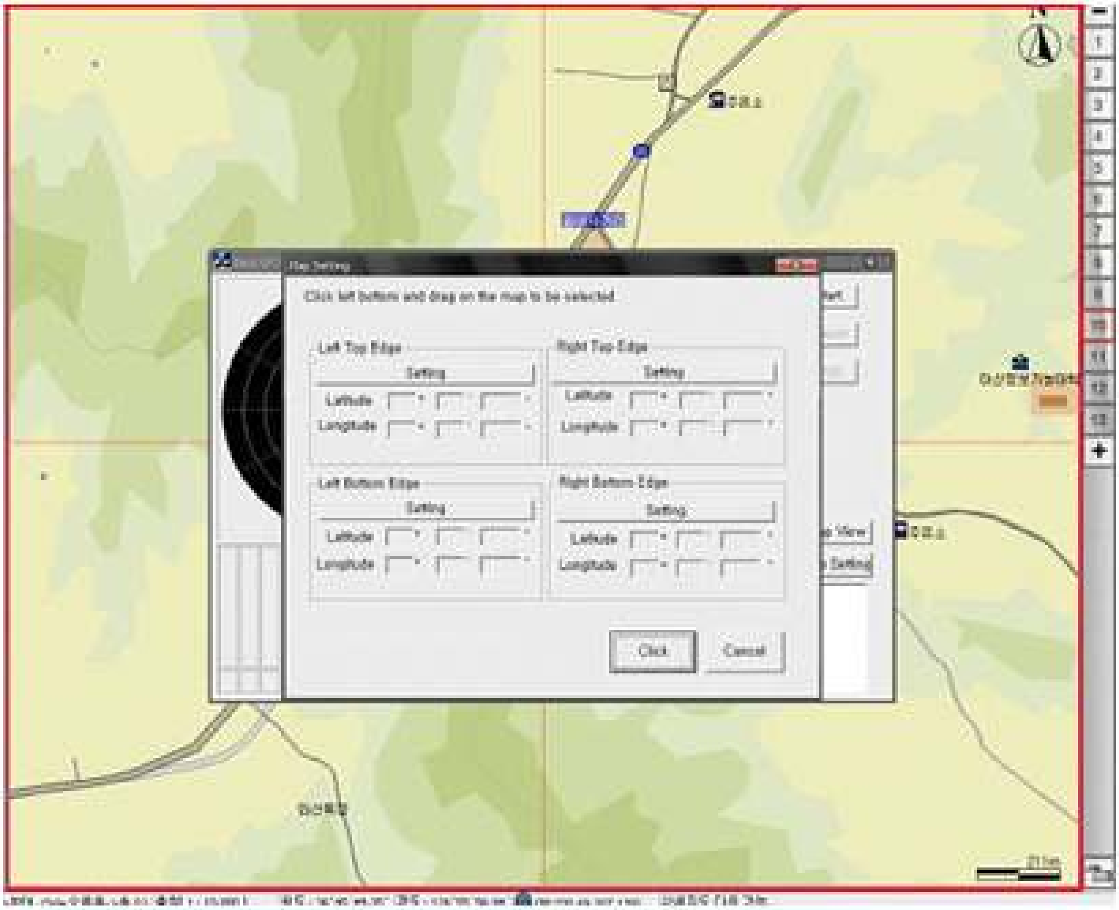
## GPS EDUCATIONAL SYSTEM TEST RESULT

The developed educational system is verified by various filed navigation test. Fig. 6 shows a navigation result. The developed GPS kit and lap-top computer installed educational software are equipped to a vehicle for field test. While the system is working in one mode, the saved map, if

### Map Setting Window

One of the outstanding features of the system is that it is independent of special map. It can use any commercial map. It has been a big program to get a map for GPS educational system because digital map is very expensive and format is often confidential. But a technique to use a cheap commercial map is devised in this paper.

Figure 5 shows map setting window of the system. The figure shows how the technique is working. First, execute the commercial map like back most map in figure. 5. If we click the 'Map Setting' button in the Main Window, the Map Setting Window is shown. Click the left button of the mouse on the Map Setting Window and drag on the commercial map to be selected. If the red box is shown like the figure, then release the mouse left button. If we click 'Setting' button for each edge, the longitude and latitude coordinate of the selected map is appeared at the bottom of the Map Setting Window. Type the longitude and latitude coordinate of four edges of the selected map and click the 'Click' button, and the shown map is saved for later use and the saved map automatically displayed if user position is into the boundary of the map.



Click left bottom and drag on the map to be selected

Figure 5 : Map Setting Window

### GPS EDUCATIONAL SYSTEM TEST RESULT

The developed educational system is verified by various filed navigation test. Fig. 6 shows a navigation result. The developed GPS kit and lap-top computer installed educational software are equipped to a vehicle for field test. While the system is working in one mode, the saved map, if it exists, is shown when the 'Map View' button is clicked. The red circle denotes present position. If the present position crosses one of the boundaries, another map, if it is already saved, is displayed automatically.

In this system, ALMAP, the popular commercial map in KOREA, is used. It costs about 10�20 USD, therefore, we can compose the educational system economically.

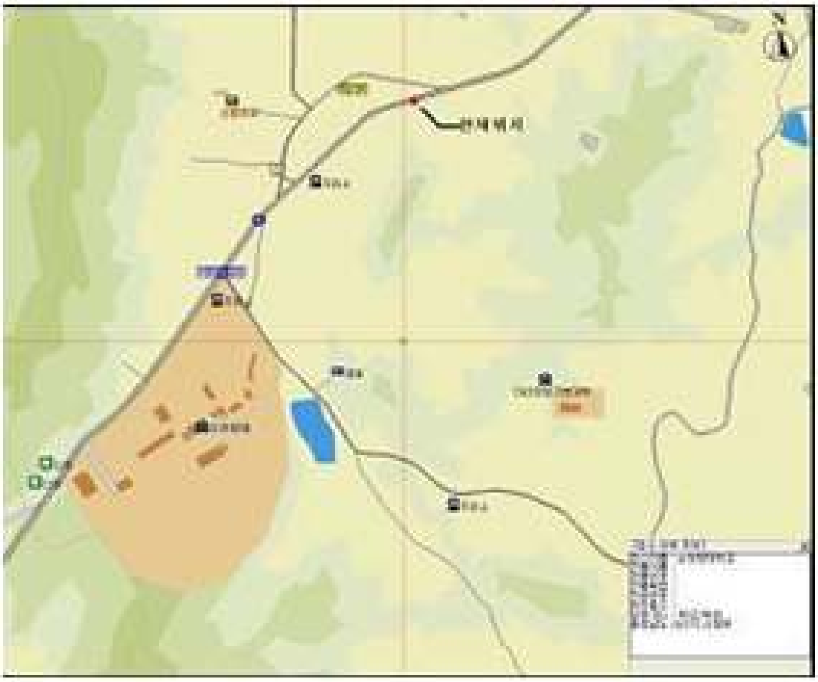


Figure 6: Navigation Test Result

## CONCLUSIONS

A GPS Educational system is developed. The system is composed of a kit and a monitoring program. The kit is composed of a GPS antenna and a board which contains a GPS receiver. It receives GPS signal through the antenna and transmit to computer through serial cable. The program, developed with MFC using Visual Studio [4] has many functions such as (1) receiving and displaying GPS signal from the kit, (2) reading and displaying a logged data from a file,( 3) displaying current position of satellites in view, (4) displaying SNR of each satellite in view by bar graph,( 5) showing current user 3-D position, (6) interfacing with ALMAP and creating map showing current user position from ALMAP, and (7) eventually enabling a user to construct his own navigation system. The developed system can be used to educate GPS basic principles and map coordinate system. Furthermore, it can be used to enable to develop other GPS related H/W and/or S/W applications. If the system is combined to other algorithm, it can be used as an algorithm educational trainer.

## REFERENCES

1. David Wells, "Guide To GPS Positioning", Canadian GPS Associates, 1996
2. Fang, B.T, The Minimum for Geometric Dilution of Precision in Global Positioning System Navigation. AIAA Journal of Guidance and Control, Vol. 10, No. 1, pp116, 1987.
3. Parkinson, Global Positioning System: Theory and Application, Vol.. I II, AIAA, 1996.Charles Petzold, "Programming Windows Fifth Edition" , Microsoft Press, 1999. 5. GPS NAVASTAR User's Overview, ARINC Research Corporation, March 1991.
4. Chang-Wan Jeon and Gerard Lachapelle, "A New TLS-Based Sequential Algorithm to Identify Two Failed Satellites", International Journal of Control, Automation, and Systems, Vol. 3, No. 2, pp. 166-172, June 2005.