Telematics Based Security System

1. A.V.Prabu 2.Baburao Kodavati 3.Tholada Appa Rao 4. E.rambabu
5. Shyam sundar tripathy
1.Lecturer in AE & IE Dept, 2.Asst.Prof in ECE Depr 3.Asst. Prof in EE Dept
4. Asst Prof in AE & IE Dept 5. Senior Training officer in Electronics Dept
1,2,3,4- Gandhi Institute Of Engg & Technology , Gunupur,Rayagada,Orissa-765022,India
5-NTTF at J.N.TATA Technical Education Center , Gopalpur,Orissa,India..
1-prabu.deva@gmail.com , 2-baburaokodavati@gmail..com ,
3-nithiamar@yahoo.in ,4- edubilliramu98@gmail.com &
5- syamtripathy1@gmail.com

Abstract--*This paper describes a new way of providing security for objects; the object can either be a file or an automotive like car, etc. The method used for providing security to objects is by creating a virtual fence around the object in such a way that whenever the object is moved out of the fence it is considered as an event and the event is notified to the user. Encryption is one of the techniques for providing security to objects, and the key used for encryption plays major role in providing security. This paper explains a new way of key generation which makes the file to be decrypted at the same location and by the same person (who knows the password) where it is encrypted, and the decrypted file is deleted whenever the fence is exited. This paper also explains a method for providing security to automobile by creating a fence around the vehicle. The engine automatically locks whenever the fence is exited and when the vehicle is used by an unauthorized person.*

Keywords: *Encryption, , Data Encryption System, HASH, RFID & GPS.*

1. INTRODUCTION

A. Security

In the computer industry, security refers to technique for ensuring that data stored in a computer cannot be read or compromised by any individual without authorization. Most security mechanisms [1] involve data encryption and passwords. Data encryption is the technique of translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system.

B. Need of Security

Computer security is necessary as the information is a strategic resource and a siginificant portion of organization budget is spent on maintaining information. Rising crime rates highten the need of people with regard to their home and car security. More people are now looking for autocop (-electronic device doing some sort of policing), for protecting their property against theft [2] and burglary.

The main idea of this paper is to make the object functioning only in a specified region and the functionality of the object is destroyed whenever the object is exited from that region. This can be achieved by using the latitude and longitude of the region as the key for the object to do its function. A Geo-fence is a virtual boundary on a geographic area. When that boundary is

DOI : 10.5121/ijwmn.2011.3212

entered or exited it can be recognized as an event and the user can be notified of that event. This event information can be sent to a mobile telephone as well as to an email account.

C. *Geofencing Applications*

- **Vehicle Tracking System:** It is an electronic device installed in a vehicle to enable the owner or a third party to track the vehicle's location. Most modern vehicle tracking system uses GPS modules for accurate location of the vehicle. Many systems also combine communication components such as satellite transmitters to communicate the vehicle's location to a remote user. Vehicle information can be viewed on electronic maps via internet or specialized software.
- **Stolen Vehicle Recovery:** A method of tracing stolen property uses a radio receiver for receiving encoded signals from a central station. When the received signal corresponds to a unique code stored at the receiver, a GPS receiver and a radio transmitter located with the stolen property are connected for a predetermined amount of time to a source of power that a GPS signal received by the receiver is processed and the position data is computed and it is transmitted to the central station.

The organization of the paper is as follows: In Section 2 we discuss the related work about the latitude and longitude information and how to create a geofence. Section 3 discusses how geofencing based security is applied for the files and Section 4 discusses how geofencing based security can be applied to automotives. In Section 5 we derive our conclusions.

II. RELATED WORK

Every region has a unique value (latitude and longitude). This unique value can be used to identify the region. The region's latitude and longitude value is unique and doesn't vary with time (the rotation of the earth).The latitude and longitude value is represented in terms of degrees, minutes and seconds. These values vary from one region to another region, but do not vary for the same location.The following graph of latitude namely Fig 2 as a function of distance shows that the latitude varies from one region to another region. In the following graph, a point 'A' is considered and from that point at a distance of nearly 100ft to right, at point 'C', we can see a change in the variation of latitude's minute field. Similarly as we move from the point 'A' to 'B' there will be a change in minute field of latitude. So the latitude (and longitude) values can be used as key to control an object.

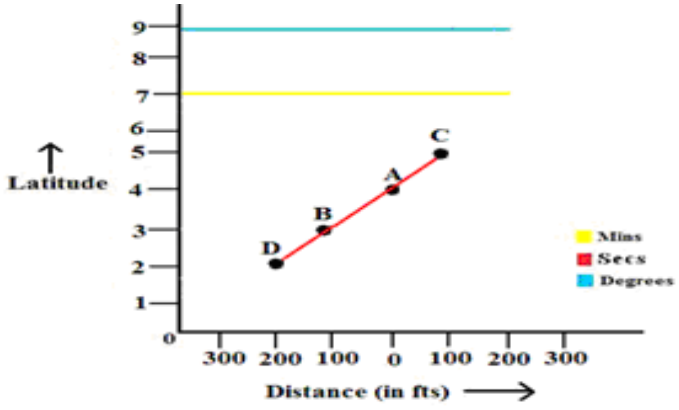

Fig 2-Variation of Latitude value with time

III. GEO FENCING BASED SECURITY TO FILES

Encryption is one of the techniques for providing the security to files. In encryption, the key used for encrypting the data plays an important role. The strength of the key increases the strength of the encryption. Hence the selection of key is vital.This paper proposes a new way for generating an input key which is given to a key generator algorithm. The key generator algorithm generates the key which is used for encrypting and decrypting the file.

A. GPS Receiver

The GPS Receiver is a device which continuously receives signal from the satellites about the latitude and longitude of a particular region, where the receiver is placed. It gets the information from the satellites in NMEA format. For latitude and longitude values to be accurate there must be at least three satellites from which the receiver should receive the information [3].

B. User Identity

User Identity is a password which uniquely identifies the person who encrypts the file. Generally it is about eight (8) alphanumeric characters to be kept secret for every individual.

C. Creating the virtual fence

The latitude and longitude values vary from place to place. Following table Table 1 gives detailed information on the variation of latitudes and longitudes from place to place.

Table 1 – Distance covered by Degree, Minute, Second values of Latitude and Longitude variation.

Latitude Longitude	Area covered (in kms)
1° of latitude	110.5743km (68.70768 miles)
1' of latitude	1.8429 km (1.1451 miles)
1"of latitude	0.0307151km (100.771 feet)
1°of longitude	111.3195 km (69.17073miles)
1' of longitude	1.8553 km (1.1528 miles)
1"of longitude	0.0309221km (101.45 feet)

From the above table it is clear that for a distance of about hundred feet, the latitude/ longitude values remain same. If we need better accuracy range, we need to have accurate GPS receiver(s). Inorder to create a fence either latitude or longitude or both should differ.

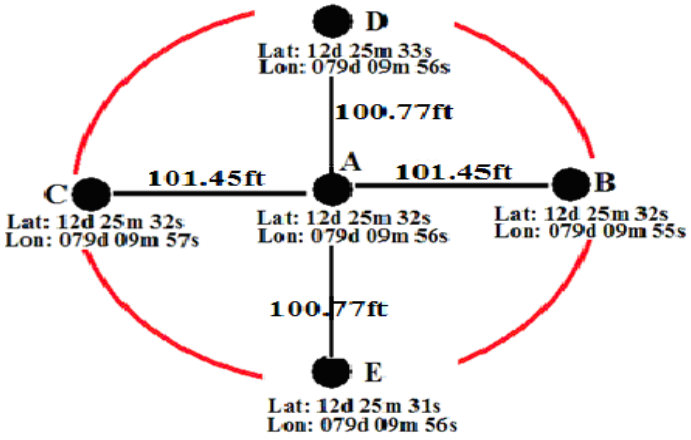

Figure 3 a- Creating a Virtual Geo fence

The above figure Fig 3a, explains the way to create a virtual fence around an object. Let us consider that an object is located at the point A (i.e., at Lat: 12d 25m 32s, Lon: 079d 09m 56s) on the earth. In order to create a virtual fence around this object, let us consider four points around this object in such a way that these points differ by only one second (1 sec) in their latitude and/or longitude values.

If we consider the point A as the object's position on the earth and consider four other points around A. Let these points be B, C, D and E. The distance between two points A and B (also A and C) is about 101 feet as we know that the distance between two longitudes when there is a variation of one second is 101 feet (approx) (from the above Table 1). Similarly, distance between the two points A and E (also A and D) is 100 feet (approx) as we see from the Table 1. So, if we join these four points we get an elliptical fence of approximately 90sq.mts area (~Π*r*r (area of circle, r is radius=100ft)) and, with in this area the value of the latitude and longitude will be same. Thus a virtual geographic fence can be created around the object, and if we use the latitude and longitude values as the key for locking of the object, the object can be localised with in an area of 90sq.mts.

D. Generation of Input Key

Once the latitude and longitude of the location is received, it must be verified whether the location lies inside or outside the fence. If the location lies inside the fence, the input key is generated by combining the latitude and longitude values received from the GPS receiver and the User Identity (password).The generated input key is given to a key generation algorithm [4], which in turn generates a key and it can be used for encrypting a file. A 64-bit input key is generated out of two keys namely LocationKey (generated from the latitude and longitude values) and UserIdentity key (generated from the User password called UIKey). For example,

Let the value of latitude be - 12 deg, 08 hrs, 15 sec

Let the value of longitude be - 79deg, 05hrs, 55sec

Let the user password is (maximum of 8 characters) - Anjali

We represent the digits of latitude and longitude using four bits. Thus, we get the following result:

12—00010010 079--000001111001

08—00001000 05--00000101

15—00010101 55--01010101

Concatenating these, yields a key (Location Key) of 52 bits (0001001000001000000101010000 01111 0010000010101010101). If we pad with twelve (12) 0s, we get a location key of length 64 bits (0001001000001000000101010000011110010000010101010101000000000000). Let us convert each character of the password into ASCII value and then convert the ASCII values into binary as explained earlier. Hence the size of UIKey is given as:

UIKey = (number of characters in password*8) bits

'A'- 01000001 'a'- 01100001

'n' - 01101110 'l' - 01101100

'j' - 01101010 'i' - 01101001

UIKey= 0100000101101110011010100110000 10110110 00110100100000000000000000

If the length of the UIKey is less than 64-bits, let us pad it also with 0s, and then perform an XORing operation between the two keys namely the location key and the UIKey to get an input key.

Input key = (locationKey) XOR (UIKey).

=1010110010011001100000001001100 1000000111100001110101111111111111

The resultant input key can be directly used for encryption or it can be given as input key to another key generation algorithm which can generate the necessary keys.The File encrypted with this key can be decrypted only by the person who encrypted the file and the location at which the person encrypted the file.

E. Encryption Algorithm

F. For out implementation, we have the used the standard DES [5] algorithm for encryption.

As with any encryption scheme, there are two inputs to the encryption function; the plain text to be encrypted and the key. In this case, the plain text must be 64 bits in length and the key is 56-bits in length.

G. Architecture Diagram

i. File Encryption

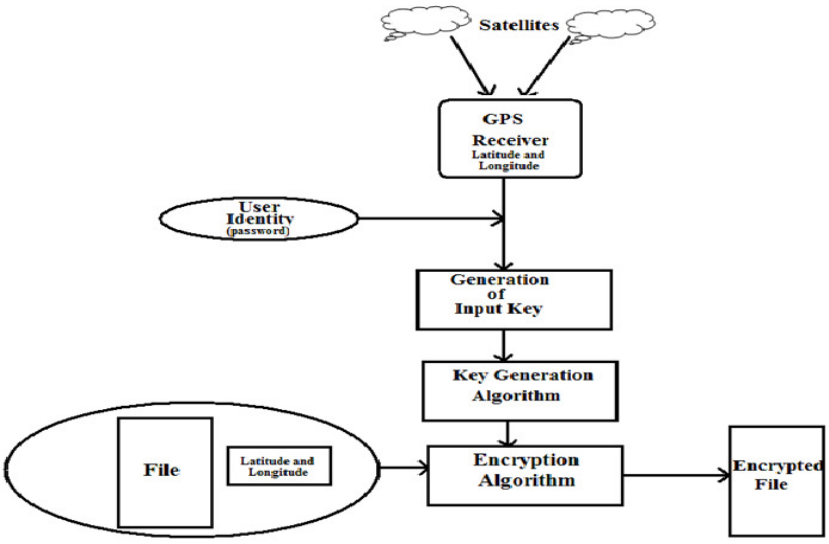

Fig 3b- File encryption using Geo fencing

During the encryption process (as shown in the Fig 3b) , the system first takes the position information (latitude, longitude) from the satellites using a GPS receiver and this position information is combined with the user password and an input key is generated. The generated input key is given to a Key Generator which generates key that can be given to the encryption algorithm. The encryption algorithm takes input a file that is to be encypted and the position information (latitude, longitude) and generates an encrypted file, which consists of the file data and the position information in encrypted form.

File Decrption:

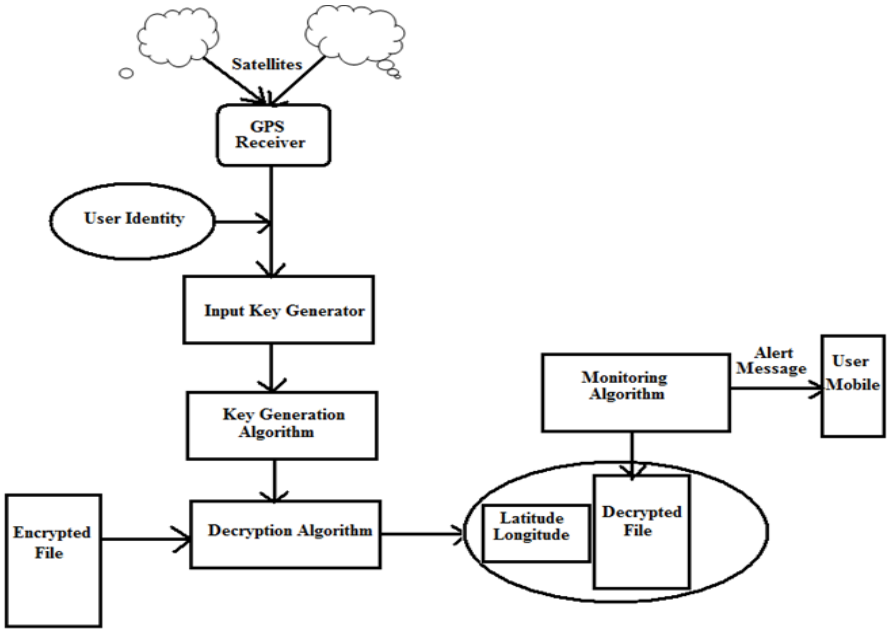

Fig 3c- File decryption using Geo fencing

H. Decryption Algorithm

The Decryption algorithm [6] transforms the cipher text into plain text and it is the reverse of the encryption algorithm.

During the decryption process, as shown in the Fig 3c, the system takes location information (latitude and longitude) from the satellites using a GPS receiver and this location information is combined with the user password and an input key is generated. The generated input key is given to a Key Generator which generates the key that can be given to the decryption algorithm. If the key generated is a valid key i.e, if the location where the file is encrypted and the person who is decrypting the file is same then the encrypted file is decrypted, and we get the original file and the location information. After the file is decrypted, the monitoring algorithm checks whether the file is within the fence by comparing the decrypted values of location information and the freshly received values from the GPS receiver. If the file exits the fence the decrypted file is deleted and an alert message is sent to the user mobile.

In the next section, we explain how the above mentioned Geofencing based technique can be extended to secure automobiles.

IV. GEO FENCING BASED SECURITY TO AUTOMOTIVES

In this section we eplain how the geofencing based security can be used in protecting parked automotives (particularly in open lawns, roadsides and streets).

Whenever a vehicle is parked at a particular location, this method takes the latitude and longitude values of the location of the parking place [7] and lock the engine. It also takes a password from the user and compares these values while unlocking the engine. The engine will be unlocked only when the both the values are matched. After unlocking the engine, this system continuously reads values from the GPS receiver and continuously compares it with the values where the vehicle was parked and locks the engine whenever there is a mismatch in the values. In order to avoid an unauthorized user guessing a password and trying to unlock an engine, we also use an RFID system. The user is expected to be tied with an RFID tag and the RFID reader is attached with the engine locking system. If the RFID tag details do not match then the engine is locked again.

A.RFID Receiver

RFID receiver is basically a radio frequency (RF) transmitter and receiver, controlled by microprocessor or Digital Signal Processor (DSP). The RFID reader, using an attached antenna, captures data from RFID tags, and then passes the data to a computer for processing.

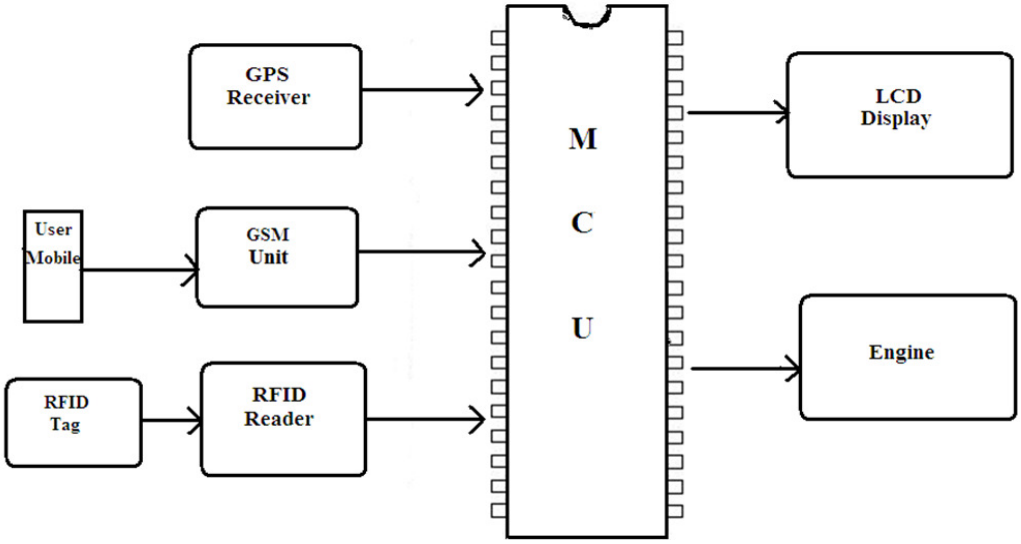

Fig 4a- Geofencing based security to Automotives

As shown in the above figure Fig 4a, while locking or unlocking, the system takes the latitude and longitude information of the place where the vehicle is parked, and also it takes password from the user. The user sends password from his mobile using an SMS (Short Messaging Service). The System allows the user to move out of the fence only if the user posses the correct RFID tag.

B. Locking Phase

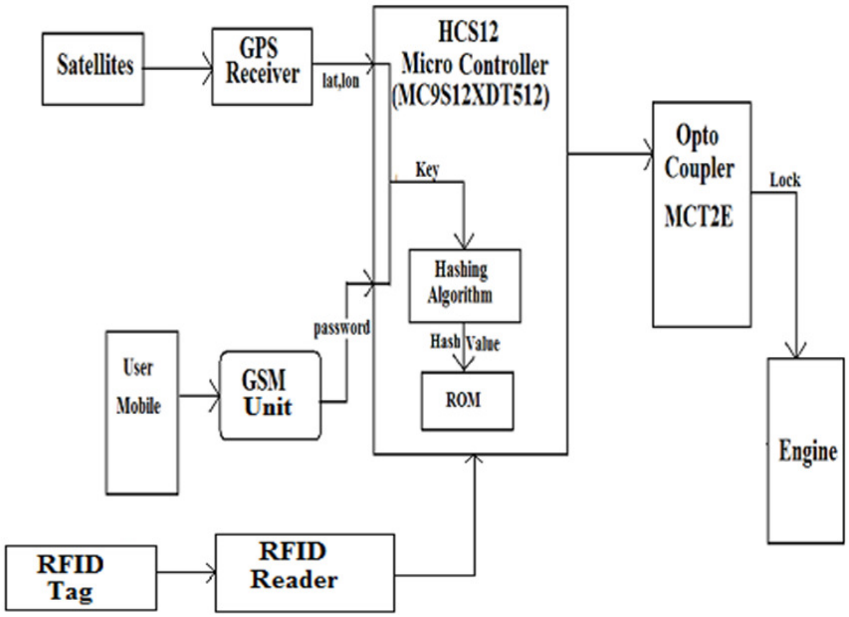

Fig 4b- Locking Engine using Geofencing

As shown in the Fig 4b while locking the car, the GPS receiver present in the car receives the latitude and longitude values of the car location [8] from the satellites and these values are sent to the microcontroller (MC9S12XDT512) (in our case). Simultaneously the user of the car sends a password through his mobile, using the SMS (Short Messaging Service) service provided, to the GSM present in the car, and then the password is retrieved from it by microcontroller. In the microcontroller the above two values are mixed and a key is generated. This generated key is then passed to a hashing algorithm which generates a hash value. The generated hash value is stored in the read only memory (ROM) of the microcontroller and using an opto-coupler (MCT2E), it converts the voltage signal to light, and switch off the battery, subsequently the engine is locked.

C. Hashing Algorithm

A Hashing algorithm generates a hash value 'h' by a function H (Hash function) of the form h = H (M); where M is the variable-length message and H (M) is the fixed length hash value.

D. Unlocking Phase

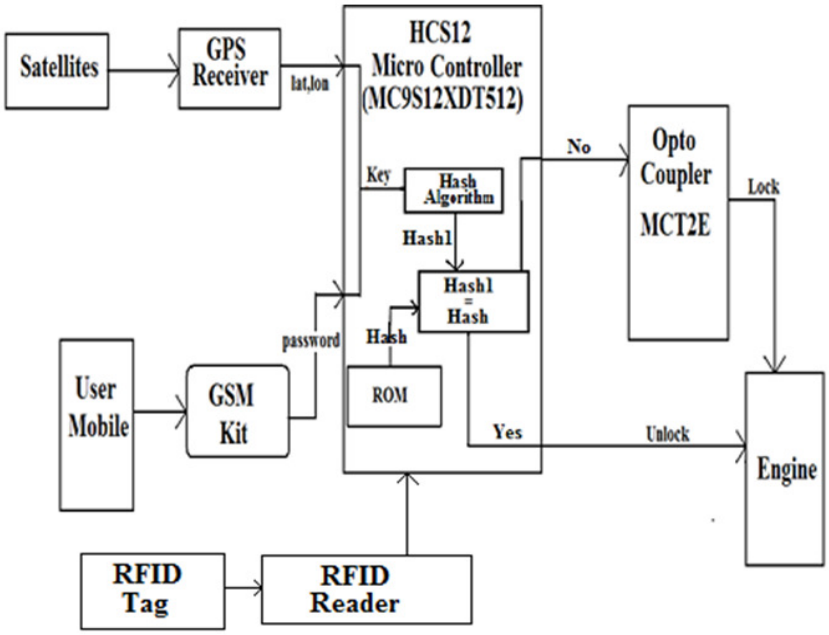

Fig 4c- Unlocking Engine using Geofencing

As shown in the above figure Fig 4c while unlocking the car, the GPS receiver present in the car receives the latitude and longitude values of the car location [7] from the satellites and these values are sent to the microcontroller (MC9S12XDT512). Simultaneously the user of the car sends a password from his mobile, using the SMS service provided, to the GSM unit present in the car. Then the password is retrieved from it by microcontroller.

In the microcontroller the above two values are mixed and a key is generated (key). This generated key is then passed to a hashing algorithm which generates a hash value (Hash1) and then compared with the hash value (Hash) stored in the read only memory (ROM) of the microcontroller and if there is no mismatch in the values then we understand that the car is

within the fence then the engine is unlocked but when there is mismatch i.e., when the car is moved out of the fence (identified by latitude and longitude values) or change in the password then using a opto-coupler (MCT2E) we send low voltage which switch off the battery and subsequently the engine will be locked.

V. CONCLUSION

This paper proposes a new way of providing security to protect objects. Usually, the basic mechanism for securing the objects is to protect it by using a password but the security mechanism fails once the password is cracked. The proposed method in this paper generates a key by using both the Geo-positioning data and user password which is used for protecting the object. Applying the Geo-position data and user password as a key is a better approach than the existing mechanisms as it creates a virtual fence around the object and the object loses its functionality whenever it exits the fence. Even if the password is cracked the geo-positioning data adds security to the object. Providing the security to automotive like car by using the proposed method is better approach as it makes the car to be unlocked only at the place where it has been locked. The RFID module ensues that only the person who parked the car can unlock the engine. If any unauthorized person attempts to use the car then it locks the engine.

REFERENCES

[1] MarkoWolf, AndreWeimerskirch, and ThomasWollinger, "State of the Art: Embedding security in vehicles", Journal on Embedded Systems, Volume 2007, Article ID 74706.

[2] J.-P. Hubaux, S. C Apkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security & Privacy Magazine*, vol. 2, no. 3, pp. 49–55, 2004.

[3] Alison Brown, JacobGriesbach and Bruce Bockius, "GPS traking location based service using wrist watch GeoZigBee Sensors", Proceddings of ION NTM, 2007, Som Diego, pp 1-10, December 2007.

[4] W.Stallings, "Cryptography and Network Security", Prentice-Hall, Englewood Cliffs, NJ, USA, 4th edition, 2005.

[5] Ingrid Verbourwhede, Frank Hoornaert, Joos Vandewalle, Hugo J. Deman "Security and performance optimization of a new DES", IEEE Journal on Solid State ciruits, vol. 23, no.3, pp 647-656, 1999.

[6] National Institute of Standards & Technology, "FIPS-46-3: Data Encryption Standard (DES)," October 1977, reaffirmed in October 1999.

[7] Sinpyo Hong, Man Hyung Lee, Sun Hong Kwon, and Ho Hwan Chun, "A Car test for the estimation of GPS/INS alignment errors", IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, VOL. 5, NO. 3, pp 208-218, SEPTEMBER 2004.

[8] Youjing Cui and Shuzhi Sam Ge,"Autonomous vehicle positioning with GPS in urban canyon environments", IEEE TRANSACTIONS ON ROBOTICS AND AUTOMATION, vol. 19, NO. 1, pp 15-25, February 2003.