*International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)*
*Volume-3 Number-1 Issue-9 March-2013*

# A Secure Mechanism to Supervise Automotive Sensor Network by Client on Smart Phone

**T R Yashavanth[1], Ravi S Malashetty[2], V R Udupi[3]**

## Abstract

***This paper presents a proposal on design of a secure client on smart phone to monitor automotive sensor network. Recently, more and more vehicles, such as BMW X5, are connected from outside via smart phone [3]. From smart phone, users can use the internet resources in automotive. Users can monitor the automotives by using their smart phones. When the automotive is moving or stolen by robber, alert information will be reported to users and users can even brake their automotive via smart phone in emergency status by sending control command to the vehicle information gateway. So client software in smart phone is required to monitor the sensor network in automotives. In order to prevent malicious attack on the client software by malicious attackers which are usually the robbers, there should be a mechanism provided to the clients which offers security by considering few criteria's like power of computation, level of security and consumption of power. This proposed method uses IDEA for the encryption of all the messages since IDEA has high level of security and suitable to implement in software and also demands on computational power is less. Record management set is being suggested for the storage of critical data which is a Java MIDlet based mechanism. Between client software and its gateway a communication management on transaction is also proposed. The verification of the key updating process is verified with model checking in UPPAAL [7].***

## Keywords

***Security, smart phone, vehicle.***

## 1. Introduction

In automotive, hundreds of sensors are networked to probe vehicle environment and vehicle running status. And all the information processing of these sensors is vital for automotive software. It is a trend that an automotive is being connected with outside via smart phone or other mobile communication devices. For example, the BMW X5 can now connect through phone to navigate the WEB, QQ etc. Also another typical application of this drive connection is that users can use smart phone to receive automotive alerting information and even control the automotives in an emergency status. These systems use sensor network and its gateway installed in the automotive, and use the smart phone as a remote client.

As the security problem in PC, the problem in automotive is even more vital. On one hand, the automotives are required to be anti-theft, safe, comfortable and convenient. On the other hand, it is should be secure, and prevented from the robbers to control the car. The software security problems are surveyed. In anti-theft sensor network is proposed, but this kind of sensor network is consisted of both off-car sensor network and in-car sensors. It is only used in parking lot. Here we concern a software security problem in a client software, with this software we can monitor the sensor network in automotive in emergency status. With this software, we must allow user to get information and control automotive remotely in emergency. But we have a void this software being maliciously used by robbers. In this paper, we present the design of this secure client in detail.

## 2. System Architecture

In vehicle there are two kinds of buses for control and infotainment specifically. The control bus connected the entire vital control unit, such as ECU, which processes sensors information and control the system via actuators. The infotainment bus connects all other devices such as GPS, dashboard, anti-theft system. Both kinds of bus are well isolated from each other to prevent the infotainment bus disturbing the control units. But some of the infotainment device needs the information from control unit .For example; the in-vehicle-anti-theft system wants to read the vehicle running status. The in-vehicle information gateway is connected in the control bus

**T.R. Yashavanth**, Computer Network & Engineering, "Jnana Sangama", Visvesvaraya Technological University, Belgaum, India.

**Ravi S Malashetty** ,Department of PG Studies,"Jnana Sangama",Visvesvaraya Technological University,Belgaum, India.

**V R Udupi ,** Prof and Head, Department of Electronics & Communication, Gogte Institute of Technology, Belgaum, India.

and the infotainment bus. This server only read data from the control bus. The data is mainly the vehicle status information, including the oil level, door lock status, and other sensor data. This gateway also reads data from the additional sensors, such as anti-firing, PIR sensor, and image sensors. This gateway is also connected with user's smart mobile phone via 3G or GSM network. In user's smart mobile phone, client software is running to accept the sensor information from the vehicle and also response to user's request to send various commands to control the car when it is in emergency, such as the vehicle is being moved by stealer, or the car is manipulated by a drunk. So this client must be secure for the vehicle owner, to avoid the car is controlled by bandits.

**Fig 1: System Architecture**

## 3. Sensor Description

Sensor identifier is composed of five parts as shown in table 1.The cabinet number means which cabinet the sensor is put in. In each cabinet, the sensor is identified with a separated serial number. The control information is decided with bit 28.When this bit is set, the sensor is companied with an actuator, and can do control to environment, such as control the ignition device or gear instrument. The sensor type is defined as the table 2.

**Table 1: Sensor Identifier**

| 28 | 27 to 23 | 22 to 16 | 15 to 8 | 7 to 0 |
|---|---|---|---|---|
| Privilege setting | Reserved | Sensor type | Cabinet number | Serial number of sensor |

We use one byte to describe the sensor property and location information.

**Table 2: Sensor Type**

| 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|---|
| 1-Valid , 0- invalid | Reserved | | Sensor locale information | | | | |

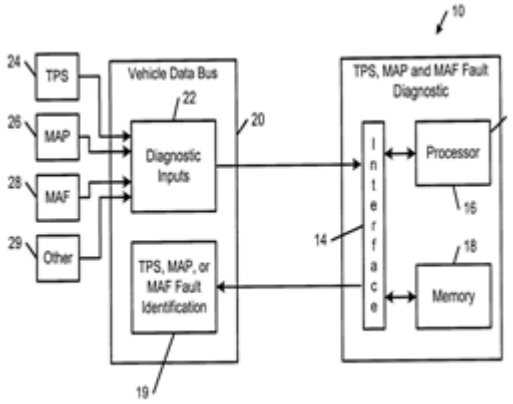


**Figure 2: Sensor Identification**

According to the invention of intake system sensor for system of fault identification has a throttle position sensor (TPS), a manifold absolute pressure (MAP) sensor, and a mass airflow (MAF) sensor. TPS, MAP sensor and MAF sensor are coupled with diagnostic controller. Faults in TPS, MAP sensor and MAF sensor are correctly identified by diagnostic controller by implementing a throttle model, a first and a second intake model. Mass airflow estimate is generated by the throttle model. First MAP estimate and second MAP estimate are generated by first and second intake model respectively. The diagnostic controller applies residual calculations on outputs of the throttle model, the first intake model and the second intake model. A first order lag filter on residual calculations is applied by diagnostic controller. In order to identify faults in TPS, MAP sensor and MAF sensor, a truth table is accessed by diagnostic controller.

For the control network in vehicle, we do not want to change the identifier information of the relevant sensors. The in-vehicle information gateway manages all the sensors in infotainment network and exchange information with control network. For the infotainment network, the gateway allocates sensor identifier for each sensor. The location description is set and passed to gateway. When received the valid sensor type and sensor location of a new sensor, the gateway will allocate one identifier automatically for the sensor.

## 4. Communication Protocol

Now the client has five types of commands corresponding to information server, as shown in table 3. We use three types of communication: SMS,

MMS and TCP/IP. Only the alert response can be optional in mms when images must be transmitted. For all three types, the sender will wait the response of the receiver in a limited time. Receivers in client will response automatically. As the SMS and MMS are store-then-forward mechanism, a secure resolution will be given in the next part.

**Table 3: Commands Send To Gateway**

| Function | Send to server op code (1byte)+ op number + '\|'+……..+op Number+'\|' | Receive from server op code (1byte) + op number + '\|'+……+op number+ '\|' |
|---|---|---|
| REGISTER | 0+password\|client port (\|'not allowed in password) | 0 resgister result, update key or not |
| Acquiction sensor location | 1 | 1+id+location+'\|'+……+id+ location+ '\|' |
| Acquisition sensor data | 2+(id+id……) | 2+id+status data+'\|'+……+id+ status data+'\|' |
| Set sensor | 3+id +'\|'+……+id+'\|' | 3+id+status data+'\|'+……+id+ status data+'\|' |
| Exit system | 4+logoff | 4 +exit result |

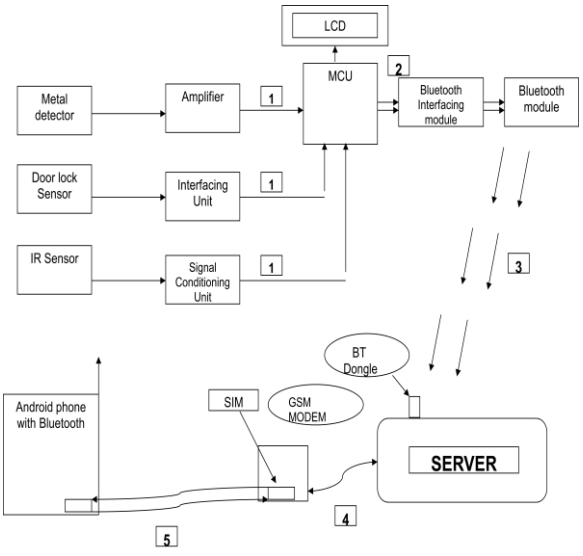


**Figure 3: General Process flow layout**

**Working**

The in-vehicle information is mainly the vehicle status information, including the oil level, door lock status, and other sensor data. This gateway also reads data from the additional sensors, such as Temperature, IR sensor. This gateway is also connected with user's smart mobile phone via 3G or GSM network. In user's smart mobile phone, client software is running to accept the sensor information from the vehicle and also response to user's request to send various commands to control the car when it is in emergency, such as the vehicle is being moved by stealer, or the car is manipulated by a drunk. So this client must be secure for the vehicle owner, to avoid the car is controlled by bandits. The users' information is authenticated with the gateway machine number, SIM card of both gateway and smart phone, and user's account. All the authentication information is stored safely by secure storage module. Only after being authenticated, the smart phone can send data to or accept data from gateway .All the communication data must be encrypted. And the encrypted data from gateway has to be decrypted efficiently in smart phone. As the SMS and MMS are store-then-forward communication, the transaction management has to be made to prohibit the communication from being intercepted.

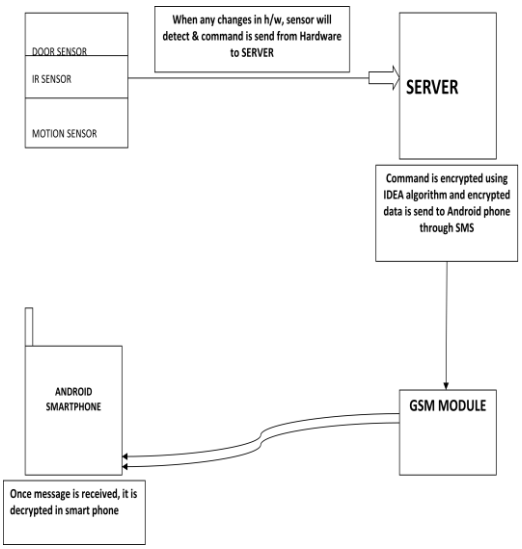


**Figure 4: Dataflow diagram**

## 5. Security Resolution

The software security problem mainly embraces the software security download into mobile phone and

the communication security between the client and server. The first one often guaranteed by the software architecture. In our client software, it is guaranteed by Java ME in java environment.

For the communication security users may confront to various hazards:

- Users may lose the smart phone;
- Someone might have stolen SIM card;
- GSM network may be jammed during communication;
- The call can be monitored by robbers.

To resolve these hazards, we use the following secure mechanism as shown in figure.
The users' information is authenticated with the gateway machine number, SIM card of both gateway and smart phone, and user's account.

All the authentication information is stored safely by secure storage module. Only after being authenticated, the smart phone can send data to or accept data from gateway .All the communication data must be encrypted. And the encrypted data from gateway has to be decrypted efficiently in smart phone.

As the SMS and MMS are store-then-forward communication, the transaction management has to be made to prohibit the communication from being intercepted.

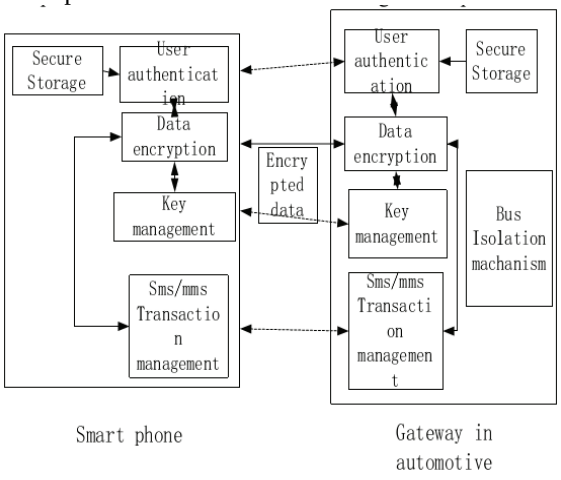


**Figure 5: Security resolution**

**Data encryption**: A valid end-to-end security mechanism is encryption. In smart phone, considering the computation capability and battery power, encryption mechanism should be secure and efficiently. The end-to-end encryption algorithm mainly embraces symmetric cryptographic algorithm and public-key cryptographic algorithm. In wireless communication, the public-key cryptographic algorithm has not been used populously as the symmetric cryptographic algorithm. There are four kinds of symmetric encryption algorithm: DES, 3DES, AES and IDEA [2]. Compared with other ones, AES and IDEA is more secure. And IDEA is more appropriate to implement with software, so we select IDEA .On the operation mode of IDEA, there are four kinds: ECB (electronic code book), CBC (cipher block chaining), CFB (cipher feedback) and OFB (Output feedback).The messages between smart phone and information server have regular format and CBC is not suited because of its weak security. OFB is also not necessary because SMS communication mechanism is relatively stable. The most efficient algorithm for SMS encryption is CBC. CBC encrypts a message within only several iterations.

**Data storage security**: For some important or privacy data, it should be stored safely. In smart phone, data can be stored in file system, record management system (RMS), or database. But the API of file system is strictly limited with signature and it is not convenient for the third part development. RMS is similar with database, and the record is valid until the MIDlet of JAVA ME is deleted. Mini database, like MYSQL, is also optional. Here we use RMS to store data. And the access privilege can be set for different kinds of data in RMS. In client, two kinds of RMS records must be stored. One is the current key, and another is the key still not confirmed. Each key is bounded with the SIM card number of information center.

**Table 4: Security Comparison**

| **Type** | **Features** | **Key length** | **Blocks no.** | **Cycles** | **Security** |
|---|---|---|---|---|---|
| DES | Data encryption , high efficient , often used for encryption of large data file | 56 | 64 | 16 | Key dependent, prone to be attacked by exhaustive search method |
| 3DES | Based on DES, encrypt data 3 times | 112<br>16 | 64 | 48 | Military level |

| | | | | | |
|---|---|---|---|---|---|
| | with different keys, highest strength. | 8 | | | |
| AES | Advanced encryption algorithm, high security level, using Rijndael. | 128<br>192<br>256 | 64 | 10<br>12<br>14 | High security level |
| IDEA | International data encryption algorithm, use 128 bit key to provide high level security | 128 | 64 | 8 | High security level |

**Key management**: Key management is also vital for the data security. When a new account is added into the information center, a key will generated according to the password and the register time. The keys are stored in RMS. And the entire keys in RMS are set to be only accessed by MIDlet APIs. This guarantees the key not being accessed by other malicious programs. In default the key will be updated every three days. This update interval can be set by users. In in-vehicle gateway each users' key, and its enable time and validity period are stored also in RMS. In our client software, we use the updating process shown in figure 3.Each time when a client logins, the gateway will determinate if a update process must start according to the last update time and validity period. When an update process starts, gateway updates key and stores it in RMS and sends this new key to client. The client then sends a confirmation message to the gateway, which then deletes the old key and sends a DON message to client, and then the client deletes the old key.

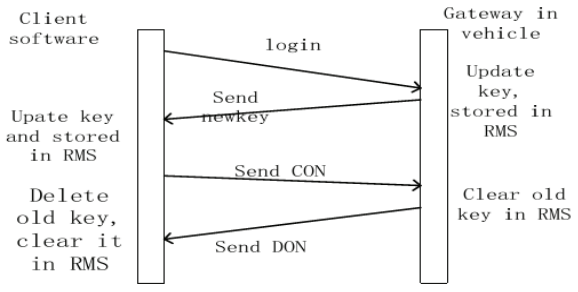


**Figure 6: Update process of key**

This process is critical. To verify the update process we modeled it in timed automata with UUPPAAL. This model consists of the client, the gateway and sync channel between then. In this model, verification on the deadlock is made. The model checking of this model also reveals that the sync of client and server has to be done via network or hardware clock; otherwise the system will be deadlock. To resolve the synchronization of transaction events, both SMS and MMS use store-and-forward mechanism. The message will be lost or be invalid because the corresponding part is not response in time.

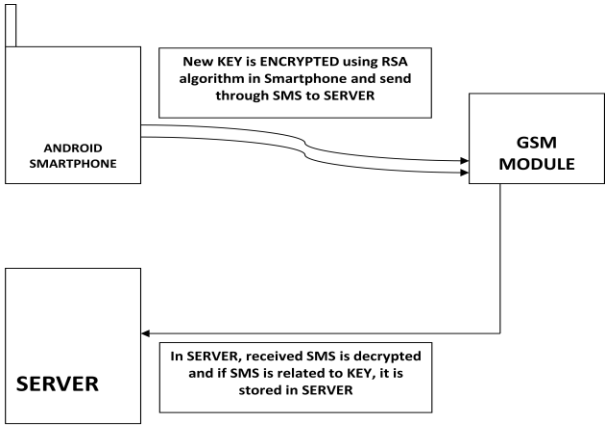


**Figure 7: Dataflow diagram for key ex-change**

To prevent the gateway or client being maliciously sent control commands or alerting messages, a transaction secure mechanism is proposed. In client software, the total number of request , noted as $C_t$ and the number of last success ,noted as Cs ,are kept and sent to the gateway when a new request is made .The client keeps the time of this request ,noted as Ts.

The gateway authenticates the request ,accept Ct and Cs ,and then sends the request result back to client companied with these two values, noted as Ct` and Cs`. After received the response from gateway, client will compare the value of Ct` and Cs` with its own Ct and Cs individually. The received time of response, noted as Tr is also kept to calculate the communication latency. The response events are accepted only if the following condition can be met.
The response events are accepted only if the following condition can be met.

$$(C_t = C_t') \wedge (C_s = C_s') \wedge (T_r - T_s \leq D),$$

D is deadline according to requirements.

## 6. Conclusion and Future work

It is a trend for automotives to connect outside via mobile devices such as smart phone. An important role is played by client software. However, the security problem in such client is critical for the automotive, even to the privacy and safe of the driver. On one hand, it is convenient and comfortable to monitor the sensor network in vehicle so as to monitor the vehicle in smart phone. On the other hand, we have to prohibit the robbers using the client software to control automotive remotely. So, security in such client is absolutely important. In this paper, we propose a design for this client software and its secure solution. In this paper we also verified the key updating process with model checking in UPPAAL. In future, we will continue to verify the other parts of this resolution and implement this design.

## References

[1] Thomas Wollinger ,Sandeep Kumar, "Fundamentals of Asymmetric Cryptography" , Embedded Security in Cars Securing Current and Future Automotive IT Applications, pp. 145-165,2008.

[2] Sandeep Kumar, Thomas Wollinger, "Fundamentals of Symmetric Cryptography", Embedded Security in Cars Securing Current and Future Automotive IT Applications, pp . 125 - 143, 2008.

[3] Christof Paar, "Embedded IT Security in Automotive Application – An Emerging Area", Embedded Security in Cars Securing Current and Future Automotiv e IT Applications, pp. 3-13, 2008.

[4] A.Bogdanov, D. Carluccio, A. Weimerskirch, T. Wollinger, escrypt GmbH, "Embedded Security Solutions for Automotive Applications", advanced Microsystems for automotive applications, pp. 177-191, 2007.

[5] Hui Song, Sencun Zhu and Guohong Cao, "SVATS: A Sensor-network-based Vehicle Anti-Theft System", In proceedings of INFOCOM, pp. 2128-2136, 2008.

[6] Marcus Heitmanm, "Security Risks and Business Opportunities in In-Car Entertainment", Embedded Security in Cars Securing Current and Future Automotive IT Applications, pp. 233-246,2008.

[7] Ki m G. Larsen1, Paul Pettersson, WangYi , "UPPAAL in a nutshell", International Journal on Software Tools for Technology Transfer (S TTT) ,Vol 1.No 1-2,pp.134-152,1997.

[8] Ward D.D, "MISRA Standards for Automotive Software", In Proceeding of Automotive Electronics, pp.5-8, 2006.

[9] Ludovic Apvrille, Rachid El Khayari, Olaf Henniger, Yves Roudier, Hendrik Schweppe, Herve Seudié, Benjamin Weyl, and Marko Wolf. Secure automo-tive on-board electronics network architecture. In FISITA'10, World Auto-motive Congress, 30 May-4 June, 2010, Budapest, Hungary, 2010.

[10] Norbert Bißmeyer, Hagen Stübing, Manuel Mattheß, Jan Peter Stotz, Julian Schütte, Matthias Gerlach, and Florian Friederici. simTD Security Archi-tecture: Deployment of a Security and Privacy Architecture in Field Opera-tional Tests. 7th ESCAR Embedded Security in Cars Conference, Düsseldorf, November 2009.

[11] Michael Glass, Daniel Herrscher, Herbert Meier, Martin Plastowski, and Pe-ter Schoo. SEIS - security in embedded ip-based systems. ATZ elektronik worldwide 1/2010, p. 36, 01 2010.

[12] D. Bailey and C. Paar. Efficient arithmetic in finite field extensions with application in elliptic curve cryptography. Journal of Cryptology, 14, 2001.

**T.R. Yashavanth** has received B.E (Computer Science & Engineering) degree from B G S Institute of Technology, Visvesvaraya Technological University, Karnataka, INDIA, with first class in 2009. Currently pursuing M.Tech (fourth sem) in Computer Networking & Engineering from Visvesvaraya Technological University, Belgaum, Karnataka, INDIA. He has 03 years' experience in teaching. His areas of interest are Wireless Sensor Networks, MANET and Cloud Computing. He has 6 papers in National and 2 papers in International Conferences to his credit. He was a reviewer for the 8th IEEE Conference on Industrial Electronics and Applications (ICIEA 2013), which will be held in Melbourne, Australia during June 2013.

**Dr. Vishwanath R Udupi,** Professor and Head of The Department, Electronics & Communication Engineering, GIT Belgaum. He has 27 years' experience in teaching, 1 year experience in industry and 12 years' experience in Research. His areas of interest are Computer Vision, Wireless Sensor Networks, and Cloud Computing. He has 13 papers in National, 22 in International Conferences and Published 8 papers in International to his credit. He has Guided 4 members for Ph.D.s and 28 Master level Projects. Professional Memberships are ISTE, CSI, SSI, ISOI & BMESI. He has got 3 awards. Interaction with Professional Institutions are BOS & BOE member for CS/ IS board in VTU, Research committee member in VTU, LIC member for VTU, BOS member for CS/ IS board in Shivaji University, Kolhapur.