Sensors & Transducers, Vol. 25, Special Issue, December 2013, pp. 197-202

www.sensorsportal.com

Sensors & Transducers

http://www.sensorsportal.com

Inspection Solution of Unlawfully Modified Vehicle by Sensor-RFID Technology

[*1] Jialiang He, [2] Peng Shen, [3] Zhiqiang Xu

[1, 2] College of Information and Communication Engineering, Dalian Nationalities University, China

[3] Communication & Media Institute of Sichuan, China

E-mail: urchin2012@sina.com; shenpeng@sina.com; starsep928@yahoo.com.cn

Received: 16 September 2013 /Accepted: 15 October 2013 /Published: 23 December 2013

Abstract: Unlawfully modified vehicles not only lead to latent security danger in transportation management, but also lead to more emissions of exhaust gas usually, it is harmful to our environment. Mandatory vehicle examination cannot be taken easily for each vehicle, so automatically and remotely indentifying whether a vehicle has been unlawfully modified or not is very necessary. In this paper, we propose an inspection solution framework of unlawfully modified by Sensor-RFID technology. In addition, sensor and RFID tags management process for vehicles and RFID security protocols are introduced detailed. *Copyright © 2013 IFSA.*

Keywords: Sensor-RFID, Vehicle Inspection, Security.

1. Introduction

Unlawfully modified vehicle has become an important problem in traffic management, the percentage of traffic accident is ascending in recent years, so it attracts attentions of traffic management department and traffic research specialist.

Unlawfully modified vehicle is that function or overload about surface, motive power system, drive line system, braking system include other key parts is over the limits of traffic laws or manufacture guidelines. Unlawfully modified vehicles not only lead to latent security danger in traffic management, but also lead to more emissions usually, it is harmful to our environment. Mandatory vehicle examination cannot be taken easily for each vehicle, so automatically and remotely verifying is very necessary. Usually, the modification of vehicle surface is recognized easily, but motive power system, drive line system, braking system is inside of the vehicle, so it is difficult to judge whether it has been over–limited modified already.

Research show that it is feasible and inexpensive to construct an intelligent traffic monitoring system based on Internet of Things [1], and the intelligent traffic monitoring system based on Internet of Things has a number of advantages such low cost, high reliability, never affected by adverse weather, all weather operations etc.

Radio Frequency Identification (RFID) is a technology which is used to identify remote objects embedded with RFID tags by wireless scanning without manual intervention RFID technology is a key enabler of the future IOT and it has a great economical potential[2], and has been used in various application domains. A typical RFID system is composed of a backend server, readers and tags. According to power supply, RFID tag is categorized into three types as follows: (1) Active tag: With built-in power supply, it is able to send information initiatively, and has higher cost to implement but with longer transmission range; (2) Passive tag: With no built-in power supply, it is used most popular because of lower cost. It comes with shorter

transmission range and more limited calculation resources and smaller storage capacity. (3) Semi-passive tag: With power supply which is merely for unit operation, its all kinds of characters are between Active tag and Passive tag. In automobiles, active tag or semi-passive tag can be used without thinking about power supply.

RFID tags and sensors are regarded as the two most important interface terminals of IoT, it has been used in the traffic management [12, 13]. In a modern automotive, there are hundreds of sensors communicating and being controlled by the electronic control unit (ECU) of the vehicle. However, the final control authority of a vehicle is mastered by the vehicle owner, so if the traffic management want to know some helpful information that maybe is unfavorable for the owner from the vehicle, it should inspect forcibly and objectively by some technology method. Sensor-RFID presents a useful function for this requirement. This information being inspected would be transmitted from sensors to a tag attached on each vehicle firstly, and traced by RFID readers that installed on the key traffic monitoring spot.

The main contribution of this paper is to propose inspection solution framework of unlawfully modified by Sensor-RFID technology. In order to implement this scheme, the related work is introduced in Section 2; enabling technologies and system design are shown in Section 3; the RFID tag management process of each vehicle is shown in Section4; the corresponding RFID security protocol is proposed in Section 5; finally, a conclusion is made in Section 6.

2. Related Work

Recently, RFID and sensor technology used in traffic management have been investigated and researched actively [7-10]. In [9], the authors present a typical application a framework of vehicle emission inspection and control through RFID and traffic lights. Automotive petrol engine emissions closely relate to air-ratio called lambda (λ) among all of the engine variables [3]. Therefore, engine emissions control is an important research topic recently [4-6]. Usually, Built-in lambda sensors which are located in the upstream and downstream positions of the catalytic converter have been installed in modern automobiles. These sensors send real-time lambda signals to the electronic control unit (ECU) of the vehicle. So the ECU can monitor the situation of the catalytic converter. In [3], a communication device is attached to the built-in lambda sensor and sends out the λ value along with the RFID tag ID to the government authority. Then the government authority can notifies and forces the vehicle owner to perform engine maintenance when the λ value of the engine exceeds the standard. Ultimately, the engine emissions can be effectively inspected or controlled by this way, so if the owner has modified over-limited motive power system, it will be detected. The solution [9] uses traffic light as key setting positions of wireless RFID reader.

In this paper, we propose a solution framework of unlawfully modified vehicle inspection by Sensor-RFID traffic light. Every vehicle must stop in front of traffic light and wait at least tens of seconds, so it is the best time to wirelessly detect the value of a specific tag that communicates with sensors. If every traffic light is equipped with a RFID reader, all using vehicles can be inspected continually.

Linear Variable Differential Transformer (LVDT) sensors are widely used in hydraulic and pneumatic mechatronic systems for measuring physical quantities like displacement, forcer pressure. The LVDT sensor consists of two magnetic coupled coils with a common core and this sensor converts the displacement of core into reluctance variation of magnetic circuit. LVDT sensors combines good accuracy with low cost [11] and is used in vehicle.

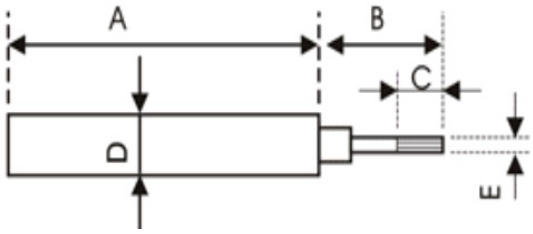

Fig. 1. System structure of LVDT sensor.

In this inspection system, considering the objective of the current application where only several kilobytes of information (few values from sensors along with a tag ID) are retrieved, RFID is suitable for its low cost and size. (1) RFID tag: for the requirements of the applications under the issues of cost, power, and size of the tags. We use semi-passive tags which have read/write functions, increased range, and can connect to built-in lambda sensors. (2) RFID reader: traffic light is an important component, it is a good place to stop a vehicle and perform wireless inspection. Firstly, the high speed of vehicles may make the RF interrogation unreliable. Secondly, it is unnecessary to inspect every vehicle continuously. It is already enough to just periodically sample and inspect. Anyway, a vehicle must eventually stop behind traffic light within a time period, e.g., a week. It is acceptable to have a weekly wireless inspection. Thirdly, considering there are several hundreds of traffic lights in a city, lower inspection rate can reduce the load of data transmission and the server calculation, making the whole inspection system more efficient. (3) Backend server: When the RFID reader receives information from a tag, the way of data transmission to the backend server may use wireless telecommunication technology such as GPRS or 3G.

3. System Design

The system design of the whole information system includes two parts: information situation and build-in RFID tag management. The information situation considers how a RFID reader on a traffic light communicates with a RFID tag built-in a vehicle. In Fig. 2, several vehicles stop in front of a traffic light but only a few RFID tag are interrogated at the same time for the reason of the effectively range of the tag. The checked value along with the tag ID of a vehicle is sent to the backend server via wireless telecommunication. If the value is different from an examination standard, the backend server will send a message to the traffic management that the vehicle maybe modified unlawfully.

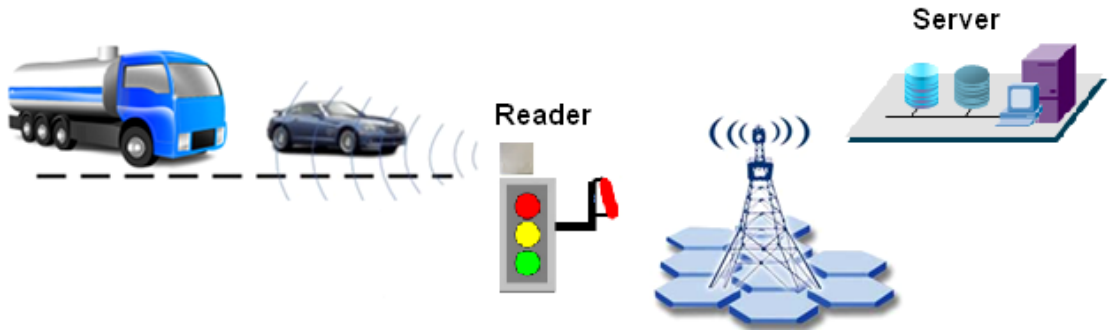

Fig. 2. Information of RFID communication.

The installation of build-in RFID tag as shown in Fig. 3. There are actually three lVDT sensors installed on the fixed edge of motive power system, drive line system, braking system. Each of them is used to evaluate if the fixed object has been moved or not. In order to measure the out value of LVDT sensor, it is necessary to connect to the RFID tag attached on the vehicle. It can be seen that only a simple wiring is enough to obtain the output value signal, which is a low voltage. This signal is then sent to the RFID tag via I2C device. Then the RFID tag is installed on the inner side of windshield for clear interrogation and future easier maintenance. The active RFID tag now acts as a wireless modem and sends out the output value from each LVDT sensor signal along with the tag ID to the reader. After forwarding to the backend server through 3G transmission, the output value signal is interpreted according to some predefined data for checking any failed cases. So the traffic management can analyze the information and perform related disposing.

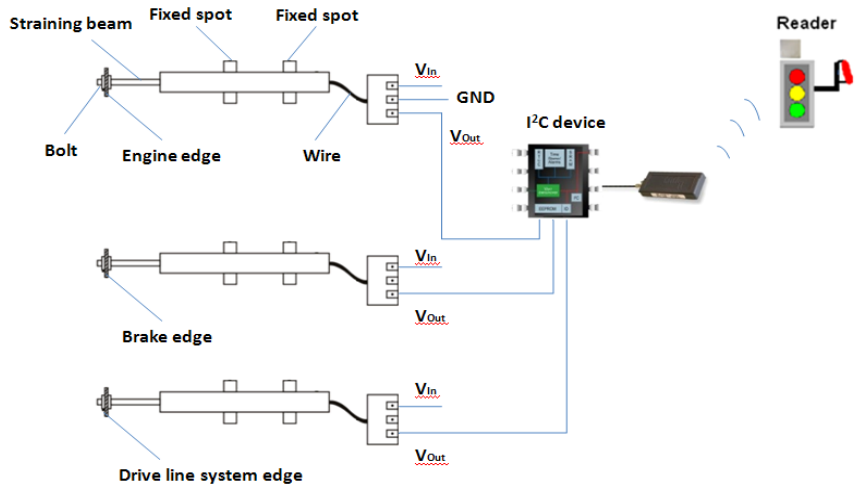

Fig. 3. Information situation of RFID communication.

In order to verify the effectiveness of this system, some experiments should be planned. In current application, the most critical part is the interrogation among the traffic light and the cars, while the issue of the data transmission from the RFID reader at the traffic light to the back-end server may be negligible because of the maturity of 3G telecommunication technology. The interrogation among the traffic light and the cars can be evaluated with two factors: effectiveness and reliability.

4. Built-in RFID Tag Management Process

Another important pre-requisite for the proposed information system is governance and legislation. Without legal support, quite a large amount of car owners will not actively install the RFID tags. In addition, RFID readers cannot be installed without government support. However, careful legislation usually takes years and this is the major obstacle preventing the implementation of the information system. Fig. 4 depicts generating process of vehicle mirror; Fig. 5 depicts key sub-system structure.

With legal support, vehicles owners maybe install RFID tags and RFID readers can be installed.

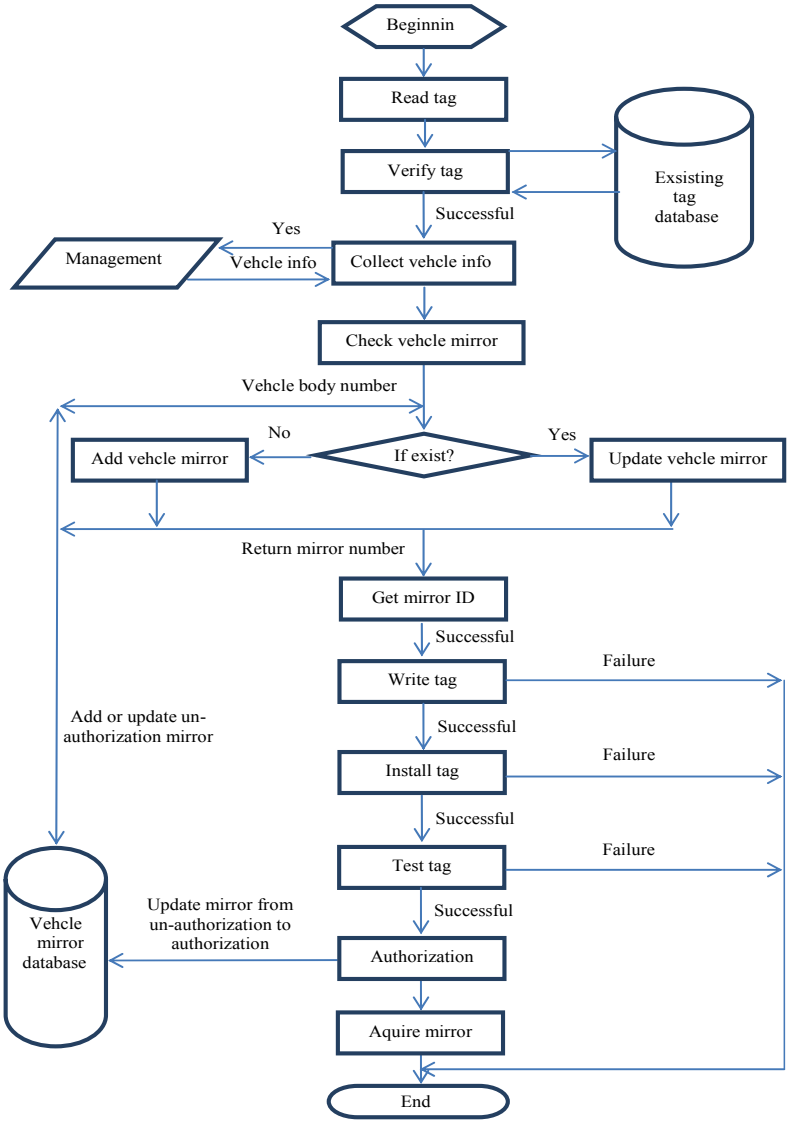

Fig. 4. Generating process of vehicle mirror.

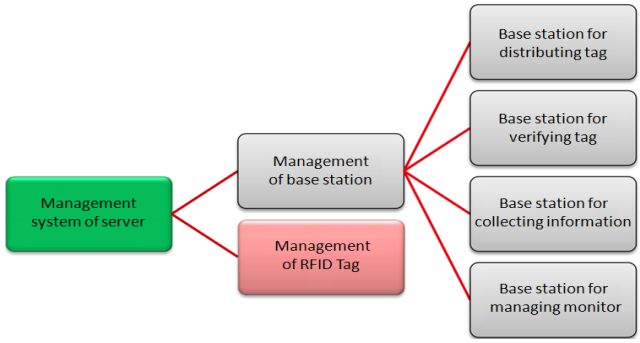

Fig. 5. Key sub-system structure.

5. A RFID Security Protocol for This Inspection System

Security is usually applied to protect important information, especially while transmitting through public area wirelessly. However, the current data transmission comprises only two simple components – tag ID, and λ reading. None of them can reveal any important information without the backend server and the database of vehicle owners. In 2011, we propose a lightweight RFID Authentication Protocol for Mobile Reader [11]. Based on this protocol, we propose a revised RFID security protocol for this inspection system which is suitable to wireless circumstance (Table 1 and Fig. 6).

Table 1. The notations used in this protocol.

Symbol	Meaning
$\oplus$	XOR operator
$\|\|$	Concatenation operator
ID	The unique identifier of a tag (The length is l)
λ	Lambda value of one vehicle
RID	The unique identifier of a reader (The length is l)
H()	An one-way hash function, H: $\{0,1\}^{l*} \rightarrow \{0,1\}^{l}$ (The length of output is l)
PRNG()	The pseudo random number generator (The length of output is l_R, usually $l_R < l$)
S_{old}	Old secret value
S_{new}	New secret value
N_T	Random number of tag
$N_{R(old)}$	Old random number of reader
$N_{R(new)}$	New random number of reader
N_{DB}	Random number of server databases

The $(i+1)^{th}$ authentication access as follows:

Step 1: The reader generates a random number N_R and query tag with N_R.

Step 2: After receiving N_R, the tag generates a random number N_T and calculates $H(N_R \oplus N_T) \oplus S$ and $H(N_T) \oplus \lambda$, then sends N_T, $H(N_R \oplus N_T) \oplus S$ and $H(N_T) \oplus \lambda$ back to the reader.

Step 3: After receiving N_T, $H(N_R \oplus N_T) \oplus S$ and $H(N_T) \oplus \lambda$ from the tag, the reader calculates $H(N_R \| N_T) \oplus RID$, and sends N_T, $H(N_R \oplus N_T) \oplus S$, $H(N_T) \oplus \lambda$, N_R, $H(N_R \| N_T) \oplus RID$ to the server. Step 4: After receiving authentication message from the reader, the server compares whether N_R matches with $N_{R(old)}$, if they match, the authentication is failed. If they don't match, the server would calculate $RID' = H(N_R \| N_T) \oplus (H(N_R \| N_T) \oplus RID)$ and search whether there exists certain RID* in table RID of the database, which could make RID' = RID*. If there exists such record, the authentication application would be considered from a legitimate reader, or authentication is failed. Subsequently, the server would calculate $S' = H(N_R \oplus N_T) \oplus (H(N_R \oplus N_T) \oplus S)$ and search whether there exists certain S_{new}* in table ID of the database, which could make $S' = S_{new}$*. If there is such record, the tag would be considered as a legitimate tag, then the server calculate $H(N_T) \oplus (H(N_T) \oplus \lambda)$ and acquire λ value firstly, subsequently generate a random number N_{DB} that could make the value which equals to $H(ID \oplus N_R \oplus N_T \oplus N_{DB})$ could not be found in column 'S_{old}' and column 'S_{new}', and calculate $H(N_R \oplus N_T \oplus N_{DB}) \oplus ID$, then send N_{DB}, $H(N_R \oplus N_T \oplus N_{DB}) \oplus ID$ to the reader, subsequently the server should update $S_{old} = S_{new}$, $S_{new} = H(ID \oplus N_R \oplus N_T \oplus N_{DB})$, $N_{R(old)} = R_{R(new)}$ and $R_{R(new)} = N_R$. If there not exists such record which could make $S' = S_{new}$*, the server should search whether there exists certain S_{old}* in table ID of the database, which could make $S' = S_{new}$*, if there exists such record, the tag would be considered as a legitimate tag, but in the last authentication access, the tag has not updated its S successfully for some reason,

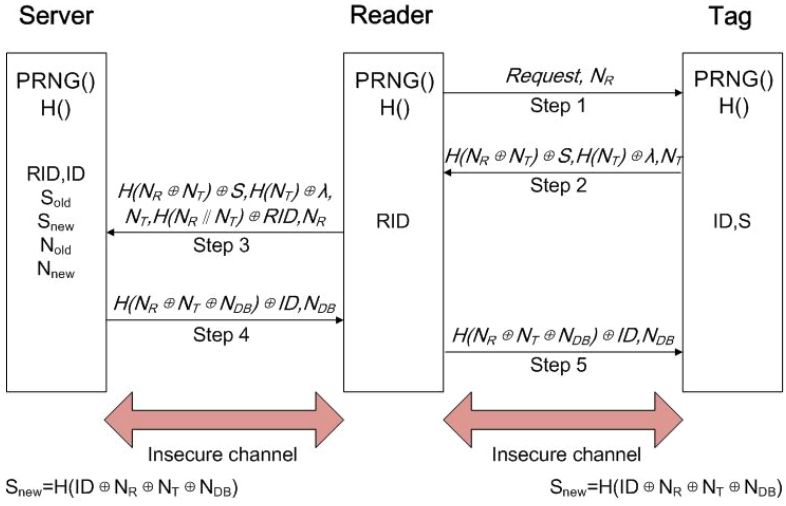

Fig. 6. The security protocol.

so the server calculate $H(N_T) \oplus (H(N_T) \oplus \lambda)$ and acquire λ value firstly, subsequently generate a random number N_{DB} that could make the value which equals to $H(ID \oplus N_R \oplus N_T \oplus N_{DB})$ could not be found in column 'S_{old}' and column 'S_{new}', and calculate $H(N_R \oplus N_T \oplus N_{DB}) \oplus ID$, then send N_{DB}, $H(N_R \oplus N_T \oplus N_{DB}) \oplus ID$ to the reader, subsequently the server should update $S_{new} = H(ID \oplus N_R \oplus N_T \oplus N_{DB})$, $N_{R(old)} = R_{R(new)}$ and $R_{R(new)} = N_R$, but S_{old} would keep unaltered. If there not exists such record which could make $S' = S_{new}*$, the tag would be considered as an illegitimate tag, the authentication is failed, failure information would be sent to the reader.

Step 5: After receiving N_{DB}, $H(N_R \oplus N_T \oplus N_{DB}) \oplus ID$ from the server, the reader would calculate $ID' = H(N_R \oplus N_T \oplus N_{DB}) \oplus (H(N_R \oplus N_T \oplus N_{DB}) \oplus ID)$ and store ID' in its memory, subsequently send N_{DB}, $H(N_R \oplus N_T \oplus N_{DB}) \oplus ID$ to the tag. After receiving N_{DB}, $H(N_R \oplus N_T \oplus N_{DB}) \oplus ID$ from the reader, the tag would calculate $H(N_R \oplus N_T \oplus N_{DB}) \oplus (H(N_R \oplus N_T \oplus N_{DB}) \oplus ID)$, If outcome equals to ID of the tag, then the object of mutual authentication achieves, the tag should update $S = H(ID \oplus N_R \oplus N_T \oplus N_{DB})$, otherwise, the authentication is failed.

6. Conclusions

In this paper, the feasibility of an information system under the concept of IoT for mandatory unlawfully modified vehicle inspection is studied in a technical viewpoint. IoT is an emerging networking concept that the pervasive or ambient things or objects are connected to provide a smart or intelligent service to make human life easier and happier. One of the enabling technologies of IoT is RFID. With RFID technology, an information system is proposed to form a wireless connection among traffic lights and vehicles. Then the unlawfully modified vehicles will be recognized. In addition, RFID tags management process for vehicles and RFID security protocols are introduced detailed.

Acknowledgements

This work was partially supported by National Natural Science Foundation of China No. 61004104; Fundamental Research Funds for the Central Universities No.DC13010215; Research Projects of State Ethnic Affairs Commission No.12DLZ001; Heilongjiang Province Science and Technology Research Grant of the Education Department No.12533002.

References

[1]. Zuo Min, Du Junping, Cloud-Processing Platform for Traffic Flow Based on Internet of Car, *China Communications,* Vol. 8. Issue 6, 2011, pp. 86-92.

[2]. He Jialiang, Ouyang Dantong, Ye Yuxin, An Efficient Lightweight RFID Authentication Protocol for Low-cost Tags, *Advances in Information Sciences and Service Sciences,* Vol. 3, Issue 9, 2011, pp. 331-338.

[3]. W. H. Course, D. L. Anglin, Automotive Mechanics, 10th edition, *McGraw-Hill,* 1993.

[4]. C. M. Vong, P. K. Wong, Engine ignition signal diagnosis with Wavelet Packet Transform and Multi-class Least Squares Support Vector Machines, *Expert Systems with Applications*, Vol. 38, Issue 7, July, 2011, pp. 8563-8570.

[5]. F. U. Syed, M. L. Kuang, M. Smith, S. Okubo, Y. Hao, Fuzzy Gain-Scheduling Proportional-Integral Control for Improving Engine Power and Speed Behavior in a Hybrid Electric Vehicle, *IEEE Transactions on Vehicular Technology,* Vol. 58, Issue 1, 2008, pp. 69-94.

[6]. C. M. Vong, P. K. Wong, W. F. Ip, Case-based Classification System with Clustering for Automotive Engine Spark Ignition Diagnosis, in *Proceedings of the IEEE/ACIS 9th International Conference on Computer and Information Science (ICIS),* 2010, pp. 17–22.

[7]. Laisheng Xiao, Zheng Xia Wang, Internet of Things: a New Application for Intelligent Traffic Monitoring System, *Journal of Networks*, Vol. 6, Issue 6, 2011, pp. 887-894.

[8]. Maria Grazia Gnoni, Valerio Elia, Alessandra Rollo, RFID technology for an intelligent public transport network management*, International Journal of RF Technologies,* Vol. 3, 2012, pp. 1-13.

[9]. Chi-Man Vong, Pak-Kin Wong, Weng-Fai Ip, Framework of Vehicle Emission Inspection and Control through RFID and Traffic Lights, in *Proceedings of the International Conference on System Science and Engineering,* Maccu, China, June, 2011.

[10]. Zhi-Yong Lu, Chao Chen, Ji Xiong, Xiao-Di Peng, The Research of Dynamic Traffic Monitoring Basing on RFID Technology in WSN, in *Proceedings of the ICTIS,* 2011, pp. 1809-1817.

[11]. Andrei Drumea, Alexandru Vasilel, Mircea Comesm, Marian Blejan, System on Chip Signal Conditioner for LVDT Sensors, Electronics System integration Technology Conference, Dresden, Germany, 2006, pp. 629-634.

[12]. Anwesha Mukherjee, Debashis De, Congestion Detection, Prevention and Avoidance Strategies for an Intelligent, Energy and Spectrum Efficient Green Mobile Network, *Journal of Computational Intelligence and Electronic Systems*, Vol. 2, 2013, pp. 1-19.

[13]. Irfan Ullah, Furqan Ullah, Qurban Ullah, Seoyong Shin, Sensor-Based Robotic Model for Vehicle Accident Avoidance, *Journal of Computational Intelligence and Electronic Systems,* Vol. 1, 2012, pp. 57-62.