DESIGN & IMPLEMENTATION OF ELECTRONIC VEHICLE IDENTIFICATION (EVI) SYSTEM

By

ENG\ MOHAMED MAHER MAHMOUD IBRAHIM

A Thesis submitted to
Faculty of Engineering – Cairo University
In partial fulfillment of requirements for the degree of
MASTER OF SCIENCE
In
Computer Electronics & Communication Engineering

FACULTY OF ENGINEERING – CAIRO UNIVERSITY

GIZA, EGYPT

2009

DESIGN & IMPLEMENTATION OF ELECTRONIC VEHICLE IDENTIFICATION (EVI) SYSTEM

By

ENG\ MOHAMED MAHER MAHMOUD IBRAHIM

A Thesis submitted to
Faculty of Engineering – Cairo University
In partial fulfillment of requirements for the degree of
MASTER OF SCIENCE
In
Computer Electronics & Communication Engineering

Under the supervision of

Ameen M. Nassar	**Hossam A. H. Fahmy**
Professor	Assistant Professor
Elec. and Com. Dept.	Elec. and Com. Dept.

FACULTY OF ENGINEERING – CAIRO UNIVERSITY

GIZA, EGYPT

2009

DESIGN & IMPLEMENTATION OF ELECTRONIC VEHICLE IDENTIFICATION (EVI) SYSTEM

By

ENG\ MOHAMED MAHER MAHMOUD IBRAHIM

A Thesis submitted to
Faculty of Engineering – Cairo University
In partial fulfillment of requirements for the degree of
MASTER OF SCIENCE
In
Computer Electronics & Communication Engineering

Approved by the
Examining Committee

Prof. Dr. Amin M. Nassar, Main Thesis Advisor

Prof. Dr. Magdi Fekry, Member

Prof. Dr. Mohamed Zaki, Member

FACULTY OF ENGINEERING – CAIRO UNIVERSITY

GIZA, EGYPT

2009

TABLE OF CONTENTS:

LIST OF TABLES:

LIST OF FIGURES:

ABSTRACT:

Transportation is one of the major sectors contributing to the growth of any country's economy. Involvement of information technology increases both efficiency and safety of such an important sector.

The objective of this thesis is to propose a single cost effective solution that merges many applications improving the efficiency and safety of the existing transportation infra-structure in Egypt. The most promising systems to do so, is the Electronic Vehicle Identification (EVI) system, we present the implementation of two applications on that system: speed limitation and electronic toll collection.

In chapter two we review the technologies used in this system, and choose one of them according to technical and non-technical considerations in developing countries like Egypt. By comparing these technologies we choose active RFID to implement our system.

Chapter three gives and overview for the system and describes its theory of operation, which is designed to overcome the constraints in a developing country like Egypt.

Chapter four presents the hardware implementation of the vehicle's tag and an analysis of the costs of this tag. The tag was implemented with a relative low cost, which is appropriate for the system deployment.

In chapter five we present the requirements for the communication protocol and we present the communication scheme between the vehicle's tag and the road-side reader.

Chapter six evaluates the performance of the system in terms of time and power consumption. The system succeeded to meet the requirements and proved to be scalable. Also we compare our system with other EVI systems and our system showed that it provides very useful applications compared to its cost.

Chapter 1: Introduction

1.1. Introduction

Transportation is one of the major sectors contributing in the growth of any economical system. Research is done to increase both the efficiency and safety of such an important sector.

Intelligent transportation system (ITS) is a term used for applying information technology to improve the performance of the existing transportation system.

Information technology has been applied to transportation systems for various purposes, for example: speed limit enforcement, traveler aiding information, toll collection, traffic modeling and many other applications. But the primary aim of all of these applications is enhancing the safety and efficiency of the transportation system available.

1.2. Traffic related technologies

Various technologies have been used to enhance the existing infrastructure of transportation systems. The following are just an example of these technologies:

Doppler radar:

Doppler radar is based on the Doppler Effect which is the phenomena of the change of the frequency of the source at the observer point according to the change of the velocity of either the observer or the source. Doppler Effect has been used in radars for detecting the velocity of objects; this by targeting the objects with an acoustic wave with a known frequency. And by measuring the deviation in frequency of the reflected signal the speed of the vehicle is being calculated.

For waves that propagate in a wave medium, such as sound waves, the Doppler Effect may occur due to the motion of either the source or the observer. For waves which do not require a medium, such as light or EM Waves, according to special theory of relativity the relative difference in velocity between the observer and the source is needed for Doppler Effect to occur. This is why the sound wave has been used in radar devices for detecting the speed of vehicles.

Inductive loops and magnetometers:

Another approach for speed detection is using two consecutive sensors on the road to detect the vehicle passage on the road. By calculating the difference in time, the speed is calculated. There are many sensors that are used for such purpose, such as an acoustic sensor (normal microphone or an ultra sonic sensor) which detects the acoustic disturbance produced by the vehicle passing in the detecting range of the sensor.

Magnetometers are used to detect the disturbance in the earth magnetic field occurring by the passage of the vehicle.

Inductive loops are used for the same purpose, as by the passage of a vehicle over a metal loop installed in the road a significant change in the inductance of this Loop occur due to the change in the material of the core which changes the frequency of an oscillator of which the inductive loop forms a part.

The inductive loops are also used in traffic lights to detect the number of vehicles waiting and accordingly the time of the traffic light is dynamically changed. But it requires to be installed during the road downtime as these loops are embedded in the road itself.

Image processing:

Cameras have been used either in radar systems, taking a photo for vehicles exceeding the speed limit or for vehicle identification and this by analyzing a photo taken to the vehicle using image processing to extract the plate number [1]. This technique is mainly known by automatic number plate recognition (ANPR). But although this technique is widely spread, it is still facing difficulties regarding the recognition algorithms; this is due to several reasons, for example: different fonts in license plate, dirt on the plate, blurring due to high speed motion, weather conditions and many other external conditions affecting the precision of the image processing.

Global positioning system:

The global positioning system (GPS) is the only fully functional global navigation satellite system. Utilizing a constellation of at least 24 medium earth orbit satellites that transmit precise microwave signals, the system enables a GPS receiver to determine its location, speed/direction, and time.

GPS has become a widely used aid to navigation worldwide, and a useful tool for map-constructing, land surveying, commerce, and scientific uses. As for the transportation field it is widely spread for navigation, applying coordinates to the vehicle's driver which is used with the aid of maps to guide drivers to their destination.

The GPS receiver can obtain these coordinates by measuring the distance between itself and three or more GPS satellites. Measuring the time delay between transmission and reception of each GPS microwave signal gives the distance to each satellite, since the signal travels at a known speed near the speed of light.

Automatic vehicle identification:

Automatic vehicle identification (AVI) refers to technology used to identify a particular vehicle when it passes a particular point. It is also known as electronic vehicle identification (EVI).

AVI can serve a range of purposes: to charge for road use, to suggest routes for drivers, to improve traffic management (such as traffic signal coordination), to detect stolen vehicles and to monitor fleets of trucks, buses, and taxis.

Wireless communication:

Wireless communication technology is used to enable vehicle-to-vehicle communication and vehicle-to-roadside communication.

Vehicle-to-vehicle communication enables voice communication between vehicles' drivers or even exchange valuable data between vehicles enabling many applications like collision avoidance.

Vehicle-to-roadside communication enables the exchange data between the vehicle and fixed or mobile units transmitting useful data concerning the road (example: road condition, speed limit for the road).

1.3. Intelligent transportation system applications

Involvement of various technologies in the transportation systems opens the door for many applications. They can be categorized as follows:

Road safety:

Safety on the road is the most important concern in the transportation systems. Speed limit enforcement and collision avoidance are forms of road safety enhancement.

Enhancing road safety does not only reduce the losses in lives and money but also implicitly increases the efficiency of utilizing the transportation infrastructure, as the reduction of accidents will lead to increase the traffic flow reducing the money losses due to traffic congestion.

Payment services:

Payment services are for example toll collection or parking fees. Involving some intelligent systems for that purpose, like electronic vehicle identification (EVI). EVI could ease the payment process for the driver also reduces the cost on the entity collecting these fees. Moreover, it will have its impact on the road efficiency, as removing barriers for collecting these fees will increase the traffic flow and reduce traffic congestion. Also applying electronic toll collection (ETC) will enable dynamic fees, and by increasing the fees during rush hours will guide the drivers to utilize the road more efficiently.

Enforcement:

Legal enforcement like speed limit and checking on vehicle and driver's license, also the weight allowed on the vehicle. New technologies are always required to do this enforcement with an efficient way.

Navigation and modeling:

Providing drivers with the suitable information for their routes, also building a traffic model which helps the transportation authorities to make a better decision about improving their transportation infrastructure. This by continuously extracting the real data about traffic status.

1.4. Objective

The objective of this thesis is to propose a single cost effective solution that merges many applications improving the efficiency and safety of the existing transportation system in Egypt.

Electronic vehicle identification (EVI) is considered the most promising technology to merge multiple applications in a single solution [2], currently EVI is commonly being used in electronic toll collection (ETC) in many countries. Such system could be extended to apply other applications once a robust communication link is established between the vehicle and the roadside. This link whether it is one way or two way communication link, it could be a building block for many applications [2]. But we will be focusing on two applications, speed limitation enforcement and toll collection, while taking into consideration the ability to extend the operation of the system for more applications.

<u>Speed limitation enforcement:</u>

In Western Europe a mere 5 km/hr decrease in average vehicle speeds is estimated to result in 25% decrease in deaths on the road [3]. So by respecting the speed limit on the road, the safety of the transportation system will highly improve.

Through the identification of a moving vehicle by road-side readers, the speed of the vehicle can be calculated by these readers. This allows the system to give a warning to the driver in case of exceeding the speed limit of the road. Moreover, if the driver does not reduce the speed, a ticket is issued against the vehicle.

The advantages of applying the speed limitation enforcement through EVI system are:

- Reduction of the cost of such application as there will not be a need for using Doppler radar which is used for speed detection on the road in Egypt.
- The ability to detect the speed of vehicles inside the city without affecting the traffic flow.
- Reduction of the number of accidents on the road as the driver will be more likely to respect the speed limitation knowing that the speed is being detected with a higher rate than the previous systems, in addition to a warning which will be given to him before charging a ticket.

Electronic toll collection:

Electronic toll collection (ETC) is a technological implementation of a road pricing concept. The system debits the accounts of registered car owners without requiring them to stop.

As for the advantages of the electronic toll collection application:

- Reduction of the cost for toll collection as it will be done automatically without the need for human interface.
- Ability of charging the vehicles for the use of main streets or bridges inside the city, while being able to make this value dynamic according to the utilization of this route. So it could be used as a tuning input to direct the people for using public transportation instead of their vehicles during rush hours, which will utilize the existing infrastructure in a better way reducing both national fuel consumption and economical losses due to traffic jam.

In the next chapter we will be presenting the various technologies that can be used for EVI or in general for vehicle-to-roadside communication.

Chapter 2: EVI technology review

Electronic vehicle identification (EVI), is considered the most promising technology to include a lot of applications in a single solution. It could be a building block for many intelligent transportation applications, although currently the most commonly used application is the electronic toll collection

Several technologies can be used for vehicle identification. In this chapter we will review these technologies

2.1. Radio-frequency identification (RFID)

With the introduction of RFID technology in 1950s, the usage of RFID has been the most common technology used for EVI.

Radio-frequency identification (RFID) is an automatic identification method, relying on storing and remotely retrieving data using devices called RFID tags or transponders. RFID tags come in three general categories: passive, active and semi-passive [4].

Passive tags:

Passive RFID tags have no internal power supply. Their power supply comes from the electrical current induced in the antenna by the incoming radio frequency signal transmitted from the reader/interrogator. This power is just enough for the CMOS integrated circuit in the tag to power up and transmit a response. Most passive tags signal by backscattering the carrier wave from the reader. This means that the antenna has to be designed to both collect the power from the incoming signal and also to transmit the outbound backscatter signal. The response of a passive RFID tag is not necessarily just an ID number; the tag chip can contain non-volatile EEPROM for storing data.

Passive tags have practical read distances ranging till about 10 cm for VHF RFID, and can reach 4m for UHF RFID [5]. The cost of the passive tags is so low that it can reach 5 US cents.

Active tags:

Unlike passive RFID tags, active RFID tags have their own internal power source, which is used to power the integrated circuits and broadcast the signal to the reader. Active tags are typically much more reliable (fewer errors) than passive tags due to the ability for active tags to conduct a "session" with a reader. Active tags, due to their onboard power supply, also transmit at higher power levels than passive tags, allowing them to be more effective in "RF challenged" environments like water (including humans/cattle, which are mostly water), metal (shipping containers, vehicles), or at longer distances. In addition active tags have the ability to store more than their ID information on the tag and able to transmit it.

Many active tags today have practical ranges of hundreds of meters, and a battery life of up to 10 years.

Semi-passive tags:

Semi-passive tags are similar to active tags as they have their own power source, but the battery is used just to power the microchip and not broadcast a signal. The RF energy is reflected back to the reader like a passive tag.

Frequency Band:

Because RFID systems generate and radiate electromagnetic waves, they are justifiably classified as radio systems. The function of other radio services must under no circumstances be disrupted or impaired by the operation of RFID systems. It is particularly important to ensure that RFID systems do not interfere with nearby radio broadcast, television and mobile radio services (police, security services, and industry).

The need to exercise care with regard to other radio services significantly restricts the range of suitable operating frequencies available to an RFID system. For this reason, it is usually only possible to use frequency ranges that have been reserved specifically for industrial, scientific or medical applications or for short range devices. These are the frequencies classified worldwide as ISM frequency ranges (Industrial-Scientific-Medical) or (short range dedicated) SRD frequency ranges, and they can also be used for RFID applications.

RFID for EVI System:

RFID is the most commonly used technology in the field of EVI [6], especially in case of using EVI for toll collection

Advantages:

- Relative low cost for tags (both active and passive).
- Low power consumption as there is no external battery needed in case of passive ID, even incase of active ID the battery life could extend till 10 Years,

Disadvantages:

- Relative short range to EVI system in case of the passive ID.
- Relative low data rate compared to other technologies (1 Mbps at maximum)

2.2. Dedicated Short Range Communication (DSRC)

DSRC is a short range wireless protocol designed for vehicle-to-vehicle and vehicle-to-roadside communication. DSRC is considered the most promising technology to be used in EVI application [7], as it opens the door to many applications in ITS field [8].

The 5.7 to 5.9 GHz (gigahertz) range of the radio spectrum has been specified by the international telecommunications union radio standards subcommittee (ITU-R) for industrial, scientific, and medical (ISM) uses.

Japan uses the 5.7 GHz bandwidth, while Europe uses 5.8 GHz. In the U.S., DSRC operates on two different frequency bands: 915 MHz (megahertz) and 5.9 GHz [9].

In the U.S the standard of the 915 MHz was developed years ago and been used in electronic toll collection, but with the requirement of new applications introduced the need of a new frequency band which is at 5.9 GHz, the following is a comparison between their characteristics[10]:

Table 1: DSRC frequency bands

Parameters	**915–928 MHz**	**5850-5925 MHz**
Spectrum	12 MHz	75 MHz
Data rate	500 Kbps	6 –27 Mbps
Possible interference	900 MHz phone; spread spectrum radio; radar	Some radar & satellite uplinks
Max . allowable range	300 Ft. (100m)	3000 Ft. (1000 m)
Channel capacity	1 to 2	7
Power consumption	2mW	2 W

Standardization is an important key in the success of any new technology, especially when it comes to large scale production and international deployment. For the appropriate standardization, all the concerned parties should be involved or at least representatives from each sector. In the case of DRSC, IEEE has involved transportation organizations, electronics and telecommunication companies and automotive companies as well in deploying the standards for DSRC operating at 5.9GHz, these set of standards defines the architecture, interfaces and message formats and goes under the IEEE 1609 family of standards for wireless access in vehicular environments (WAVE). These set form the IEEE 802.11p standard which is a modification on IEEE 802.11a standard (Wi-Fi) with 10 MHz wide channels instead of 20 MHz channels and half the data rate to be adopted for vehicular wireless communication [11].

IEEE 1609 for WAVE, approved by United States Department of Transportation (USDOT) in 2004, consists of four standards:

- IEEE P1609.1—Resource Manager:

  This describes the key components of the WAVE system architecture and defines data flows and resources at all points. It also defines the command message formats and data storage formats that must be used by applications to communicate between architecture components, and it specifies the types of devices that may be supported by the OBU resident on the vehicle or mobile platform.

- IEEE P1609.2—Security Services for Applications and Management Messages:

  This defines secure message formats and processing. This standard also defines the circumstances for using secure message exchanges and how those messages should be processed based upon the purpose of the exchange.

- IEEE P1609.3—Networking Services:

  This defines network and transport layer services, including addressing and routing, in support of secure WAVE data exchange. It also defines WAVE short messages, providing an efficient WAVE specific alternative to IPv6 (Internet Protocol version 6), which can be directly supported by applications. Further, this standard defines the Management Information Base (MIB) for the WAVE protocol stack.

- IEEE P1609.4—Multi-Channel Operations:

  This provides enhancements to the IEEE 802.11 Media Access Control (MAC) to support WAVE operations.

In the United States and Canada the DSRC should operate in 7 separate channels each of 10MHz band From 5.855 to 5.925 GHz, while in Europe 2 channels are allocated of 10MHz also: at 5.795 and 5.805 GHz [10]

DSRC for EVI systems:

Advantages:

- Relative long range compared to RFID.
- Relative high data rate.
- Standardization.

Disadvantages:

- Requires high power for transmition which requires a connection to the vehicle's battery.
- Relative high cost for each modem.[10]

2.3. Bluetooth

Bluetooth is an industrial specification for wireless personal area networks (PANs). It is designed to replace wired connectivity between different personal electronics over a secure, globally unlicensed short-range radio frequency which is in the 2.4 GHz ISM (Industrial Scientific Medical) band. The Bluetooth specifications are developed and licensed by the Bluetooth special interest group.

There are three different classes of Bluetooth; these classes are categorized according to their maximum permitted power and range [12]:

Table 2: Bluetooth classes

Class	Maximum Permitted Power	Range
Class 1	100 mW (20 dBm)	~100 meters
Class 2	2.5 mW (4 dBm)	~10 meters
Class 3	1 mW (0 dBm)	~1 meter

Bluetooth data rate differs according to the protocol version that is being used, for version 1.2 data rate can reach 1Mbps while for version 2.0 it can reach 3Mbps

Bluetooth divides its frequency band which is the 2.45 GHz band into 79 channels (each 1 MHz wide) and uses a modulation technique called spread-spectrum frequency hopping to overcome interference. In this technique, a device randomly chooses frequencies within a designated range, and switches from one channel to another on regular basis. In the case of Bluetooth, the transmitters change frequencies 1,600 times per sec. Thus it is unlikely that two devices use same channel at the same time, and even they do, the interference lasts only for a tiny fraction of a second.

Bluetooth for EVI system:

Advantages:

- Appropriate range compared to RFID.
- Relative high data rate.
- Standardization.

Disadvantages:

- Requires high power for transmition which requires connections to the vehicle's battery.
- Relative high cost for each tag.

2.4. Global System for Mobile (GSM)

Global system for mobile communications (GSM) is the most popular standard for cellular networks. GSM networks operate in four different frequency ranges. Most GSM networks operate in the 900 MHz or 1800 MHz bands. Some countries in America (including Canada and the United States) use the 850 MHz and 1900 MHz bands because the 900 and 1800 MHz frequency bands were already allocated.

In the 900 MHz band the uplink frequency band is 890–915 MHz, and the downlink frequency band is 935–960 MHz. This 25 MHz bandwidth is subdivided into 124 carrier frequency channels, each spaced 200 kHz apart. Time division multiplexing is used to allow eight full-rate or sixteen half-rate speech channels per radio frequency channel. There are eight radio timeslots (giving eight burst periods) grouped into what is called a TDMA frame. Half rate channels use alternate frames in the same timeslot. The channel data rate is 270.833 kbit/s, and the frame duration is 4.615 ms [13].

The transmission power in the handset is limited to a maximum of 2 watts in GSM850/900 and 1 watt in GSM1800/1900.

GSM for EVI system:

Advantages:

- Existing infrastructure.
- Standardization.

Disadvantages:

- Requires high power for transmition which requires connection to the vehicle's battery.
- Relative high cost for each modem.
- Not precise in case of applying speed limitation enforcement as the coverage could extend to tens of kilometers.

Although using GSM does not seem to be suitable for the link between the vehicle and the road side readers, it could be considered for the link between the road side units and the control center, the power source in this case could be land line electrical supply or solar cells.

2.5. Considerations for deploying EVI systems

Before deploying an EVI system, there are some technical and non-technical [14] points that need to be taken into consideration

Installation:

Some of the EVI technologies proposed use an on-board device which is powered up by the vehicle’s battery (example: DSRC on-board unit) [15]. But for applications like speed enforcement, depending on the battery of the vehicle as a power supply of the vehicle’s unit will make this unit subject to tampering by disconnecting the power supply. To prevent such actions, the on-board unit should be independent of any external power supplies.

Cost:

The EVI system is divided into two parts: the EVI tag which will be installed within each vehicle and the infra-structure including the readers on the road, the traffic control center and the link between them. To face the minimum public disapproval, the EVI tag installed in the vehicle should be cheap enough for each driver to buy it at the license renewal time.

Road infra-structure:

In developing countries, many roads are not connected to any communication networks or even to electrical power networks. The readers on the road side should be able to communicate with the command center for transferring data and they should be also able to operate with an independent power source.

2.6. Evaluation of technologies for EVI System

To choose a technology of an EVI system in developing countries like Egypt, we need to consider having a low cost vehicle’s tag which is independent of external power source. Cai et al [16] and Guo et al [17] reviewed some of technologies for EVI system (RFID, GSM, GPS and DSRC), from these reviews, RFID is the most appropriate according to these criteria as its tag can be implemented with low cost with low power consumption.

A passive RFID tag does not require a power source as the power source in this case is provided by the reader. An active RFID tag requires a power source which could be a battery in our case to be independent from the vehicle as mentioned before. The envisioned speed limitation application requires a long range of coverage on the road (~100 m) so as to be able to detect the vehicle from a reader mounted on the roadside. Such a range cannot be achieved with passive RFID. Hence, we decided to have an active RFID in our system for the vehicle unit.

An important consideration is the battery life time. It should be long enough to be changed only at the license renewal at the transportation authority.

Chapter 3: System Architecture

3.1. EVI System Overview

In this section we will review the system architecture for the EVI System. The System can be divided into three main Units:

- The tag installed in the vehicle.
- The reader on the Road.
- The traffic control center.

There should be two communication links between these three units:

- Communication link between the tag and the reader.
- Communication link between the reader and the traffic control center.

3.1.1. Tag – Reader link

As mentioned before, this link uses active RFID. The point now is to decide whether this link should be a two-way communication link or one-way communication link. A one-way communication link can be implemented by having the tag transmitting its ID periodically while the reader is only receiving. The advantage of making a one-way communication is to lower the cost of the tag which is the most important unit to be considered in term of cost. According to the current hardware prices [18], the use of one-way communication devices could reduce the cost to about 40%. However, a two-way communication has the following advantages:

- The tag can only transmit in case of receiving a request from the reader. Otherwise, it will be in a sleep mode, reducing its power consumption and hence increasing the battery lifetime.
- The system may be used as a building block for other future applications (example: navigation, road safety messages, etc), which are easier to implement using two-way communication links.
- The possibility of warning the driver for exceeding the speed limit in the speed limitation application.

3.1.2. Reader – Traffic control center link

The link between the reader and the traffic control center is needed so that the control center could charge the tickets in the case of speed limitation enforcement application. That link can also be used in future applications (such as navigation) to acquire data and send useful information to the driver. In main streets within the city and nearby highways, this link may use a wired connection. The wires may be laid especially for this application or to reduce the cost, the existing infra-structure of power lines (via power line communication) or the infrastructure of telephone lines (via TCP/IP for example) may be used. However, as mentioned before, many rural highways in developing countries do not have connections to wired communication networks.

The only communication network that may exist at these roads is the GSM network [19]. In such cases, data can be transferred through GPRS modems attached to the readers. The disadvantage of using a GSM network is that it belongs to the private sector in most countries. Such a solution exposes critical traffic information to a private sector company. In addition, it is vulnerable to market pricing fluctuations which may affect the running cost of the system.

An alternative solution is to use a special microwave link between each reader and the control center. Such a solution would be of a much higher cost when compared to using the existing GSM network. That choice should be handled by the traffic authority.

Whether on land lines, on GSM networks, or on microwave links, to maintain the privacy and integrity of the transmitted information, some level of encryption must be used.

Instead of instantly sending the information from each reader and having as many active communication channels in the system as there are readers, the system may be designed for a lower cost by using another solution. The data could be kept on a storage unit attached to each reader then collected periodically by sending a special command to the chosen reader to download and erase its data.

The previous solutions (land lines, GSM, microwave links, and data storage) are varying in their cost and performance. The choice of the solution translates to different quality of services. This choice should be up to the traffic authority to make. For the purpose of our project, we wanted to maintain a low cost while still providing the rural areas with a secure and decent quality of service. We wanted to be able to operate even in the absence of a full coverage of GSM networks to the whole road. A compromise between all the previous solutions is achieved by connecting the control center with only the readers where the communication network already exists (we call these the gateways). The other readers communicate with the control center by sending their messages via the connected readers (the gateways). The tag installed in the vehicle is used to forward the messages between the two types of readers. In such a scheme the latency of the GSM network or the microwave link will not be considered, as the speed calculation will not be calculated by the control center, this will be discussed in details in the next section.

3.2. System operation description

As mentioned before in the previous section, the primary applications for our EVI system will be speed limitation enforcement and electronic toll collection. For such applications multiple readers should be located on the streets inside the city and on the highway. Each of these readers should be having a unique ID and covering a certain area in such a way that these coverage areas are not overlapping.

For the speed limitation enforcement application, when a vehicle passes through the coverage area of a certain reader, the reader will request the ID of the vehicle, which in our case is its VIN (Vehicle Identification Number). The VIN is a unique number for each vehicle given by the vehicle's manufacturer.

The vehicle will reply by its VIN and then the reader will acknowledge receiving the VIN of the vehicle.

On receiving the acknowledge signal, the vehicle will store the ID of the reader, stop replying to this reader, and start calculating time till it reaches the next reader. When it receives another request with a different reader ID, the tag will reply to this request with its VIN, the previous reader ID, and the time calculated.

Each reader has a calibration table containing the distances between itself and the neighboring readers. Upon receiving the information from the tag, the second reader calculates the speed of the vehicle and compares it to the road speed limit. If the speed limit is exceeded, the reader will check if this vehicle had a previous warning or not through a flag in the message sent by the tag, if a warning was previously given then a ticket will be issued to the vehicle for exceeding the speed limit. Otherwise in the acknowledge message, a warning flag will be raised, which will be checked by the next reader. Furthermore, an audio warning (for example a beep) is given to the driver to indicate exceeding the speed limit on this road. The acknowledge message replaces the last reader ID with the new one and resets the timer.

A good advantage of our scheme where the calculation of the vehicle speed is done by a timer in the tag is that there is no need for any timing synchronization between the readers.

When the reader realizes that a certain vehicle should be given a ticket, the reader either sends this information to the control center directly in case of being a “gateway” reader, or it raises a “ticket” flag in the acknowledge message to the tag. This message will be stored in the vehicle’s tag and checked by the next readers till it is sent by a “gateway” reader and erased from the tag by the acknowledge message from the gateway reader. All the other (non-gateway) readers do not reset the “ticket” flag if it is already set.

The following are flow charts for the operation of both the vehicle’s tag and the roadside reader:

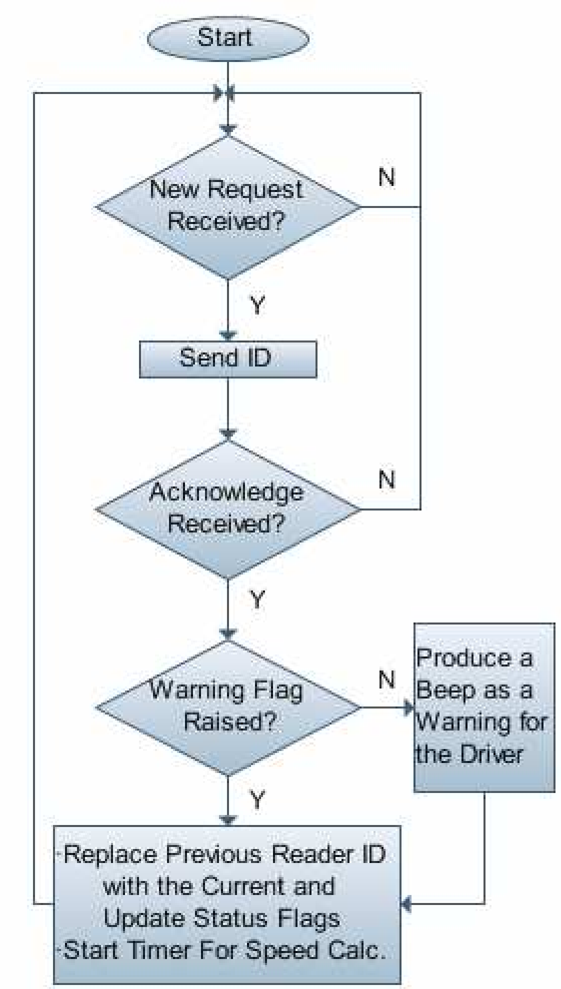
Start
New Request Received?
N
Y
Send ID
Acknowledge Received?
N
Y
Warning Flag Raised?
N
Produce a Beep as a Warning for the Driver
Y
-Replace Previous Reader ID with the Current and Update Status Flags
-Start Timer For Speed Calc.

Figure 1: Vehicle's tag operation

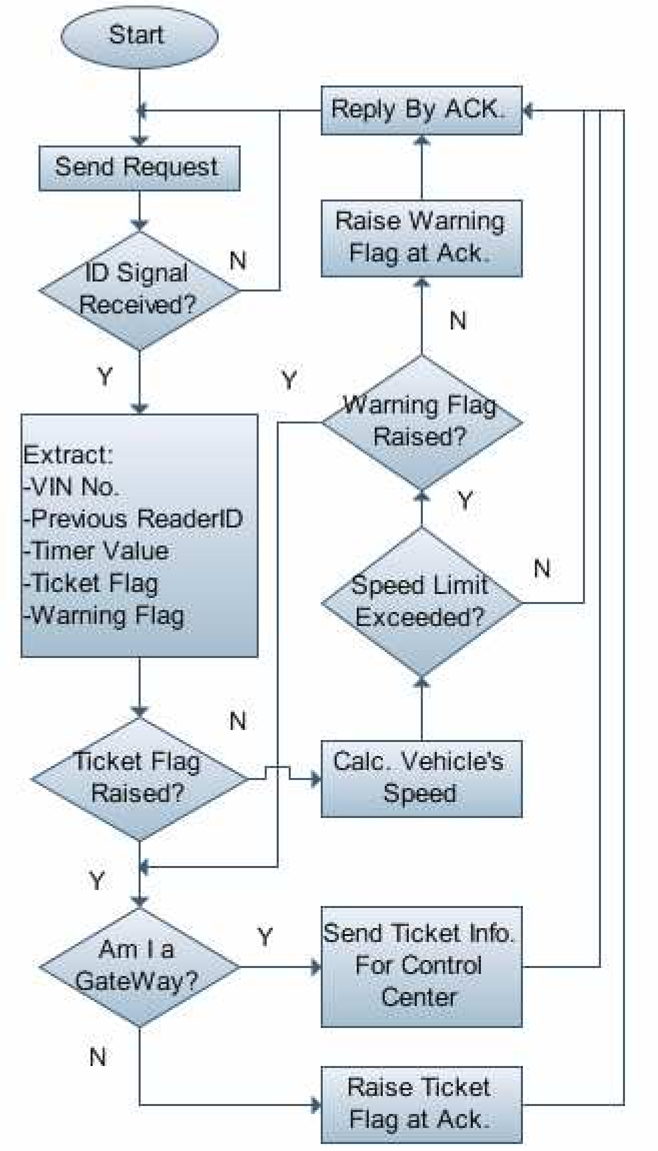

Figure 2: Road-side reader operation

As for the toll collection application, it is easily implemented by placing a reader at the position considered as the toll gate and by identifying the VIN of the vehicle as described before. The driver will either pay when renewing the license or a SIM card reader can be attached to the tag where the driver can insert a charged SIM card to pay for the road fees. Again the choice of the way of payment depends upon the quality of service which will be the decision of the authorities responsible. But it must be taken into consideration that using an attached SIM card reader increases the cost of the tag. When the driver pays the cost of the tag at license renewal time, the addition of the SIM card reader may be proposed as an option. The default of the system is to send the vehicle's VIN and charge its records at the control system. If the tag has an attached SIM card reader and the card has enough money charged to pay the required fees, the amount is deducted and an indication of the payment is sent to the control center to remove the charges. Such an operational mode is flexible enough to allow the drivers to move along without worrying much about the current amount available in their SIM cards.

3.3. Reader's antenna position and pattern

There are two parameters that should be considered during the design of the system concerning the reader's antenna, which are the position of the antenna on the road and the pattern of this antenna.

These two parameters are related to each other, as the decision of both the position and the pattern in most cases should be based on covering the maximum possible area from the road with the minimum power consumption. But in other cases it could be based on having a specific coverage area to be able to know the position of the vehicle identified, these cases for example is like having a reader on a bridge, in such case we need to identify whether the vehicle is on the bridge or under. So it is possible to offer different types of readers with different antenna pattern so as to ease the choice of their position.

3.4. Legal Considerations

It is important to have a proof for the speed ticket, to be provided to legal authorities in case the driver denied this ticket, also to be sure that the system didn't issue that ticket by mistake, this could be achieved by adding a camera sensor at the gateways that will take a picture of the vehicle in its reading zone when receiving a ticket flag.

Chapter 4: Hardware Design & Implementation

This chapter describes the design and the implementation of the tag H/W. As mentioned before at chapter 2, RF tag will be used for the communication between the vehicle and the roadside.

4.1. Design considerations

For the design of the tag H/W the following points should be taken into consideration:

- The cost of the vehicle's tag should be as low as possible, so as to be able to oblige the driver to buy this tag during renewing the license while facing minimal public disapproval.
- The tag could operate in a range which can reach 50m, to be able to cover an acceptable area.
- The tag should operate with a power source independent from the vehicle, to ease the installation and minimize the possibility of tampering.
- In this case if the power source is a battery, the battery life should be long (~3 years, to be able to change by the authorities at license renewal).

4.2. Operating Frequency

The choice of the frequency band of the system operation should be done carefully so as to minimize any possible interference with other systems. In each country there is a governmental authority for coordinating the frequency allocation inside the country besides setting the constraints for the transmission (i.e.: power of transmission, range … etc) at these frequencies. The ISM (Industrial, Scientific and Medical) bands are frequency bands allocated in each country for the industrial, scientific and medical applications without the requirement for the approval of the communication authority. These bands differ from one country to another according to their region. Egypt is allocated at region 1 [20] which include Africa and the Middle East, Europe and Part of Asia.

In this thesis we will be using the 2.4GHz frequency band for the operation of the RF Link between the Vehicles' Tag and the Road-Side Reader. This frequency band is an ISM Band and its range is from 2.400–2.500 GHz (centre frequency 2.450 GHz) [21] this frequency band is commonly used in Bluetooth, WiFi, ZigBee …etc.

Unfortunately, mutual interference between the wide ranges of ISM applications is not uncommon in this frequency range, but most of these applications are domestic and the EVI applications will all be applied on the road. However this thesis is only a proof of concept and it would be better to operate in another frequency band dedicated for such applications on realizing such a system to avoid any possible interference. And in this case it is better to use the frequency band of 5.8GHz (5.795 – 5.815 GHz) which is being used for DSRC in Europe as mentioned before.

4.3. Tag implementation using CC1010

The first trial for implementing the vehicle's tag was using CC1010. CC1010 is a single-chip UHF transceiver from Chipcon with an integrated high performance 8051 microcontroller, it has the following features:

- 300-1000 MHz RF Transceiver.
- Very low current consumption (9.1mA in RX).
- High sensitivity (typically -107 dBm).
- Programmable output power up to +10 dBm.

- Data rate up to 76.8 kbps.
- Very few external components.
- Analog received Signal Strength (RSSI) Indicator.
- 32 kB Flash, 2048 + 128 Byte SRAM.
- channel 10 bit ADC, 4 timers / 2 PWMs, 2 UARTs, RTC, Watchdog, SPI, DES encryption, 26 general I/O pins
- 2.7 - 3.6 V supply voltage

For testing the RF link CC1000 from Chipcon was used. Which is the same transceiver used in CC1010 but without the microcontroller processor. The figures below show the circuit schematic and implementation for CC1000 circuit:

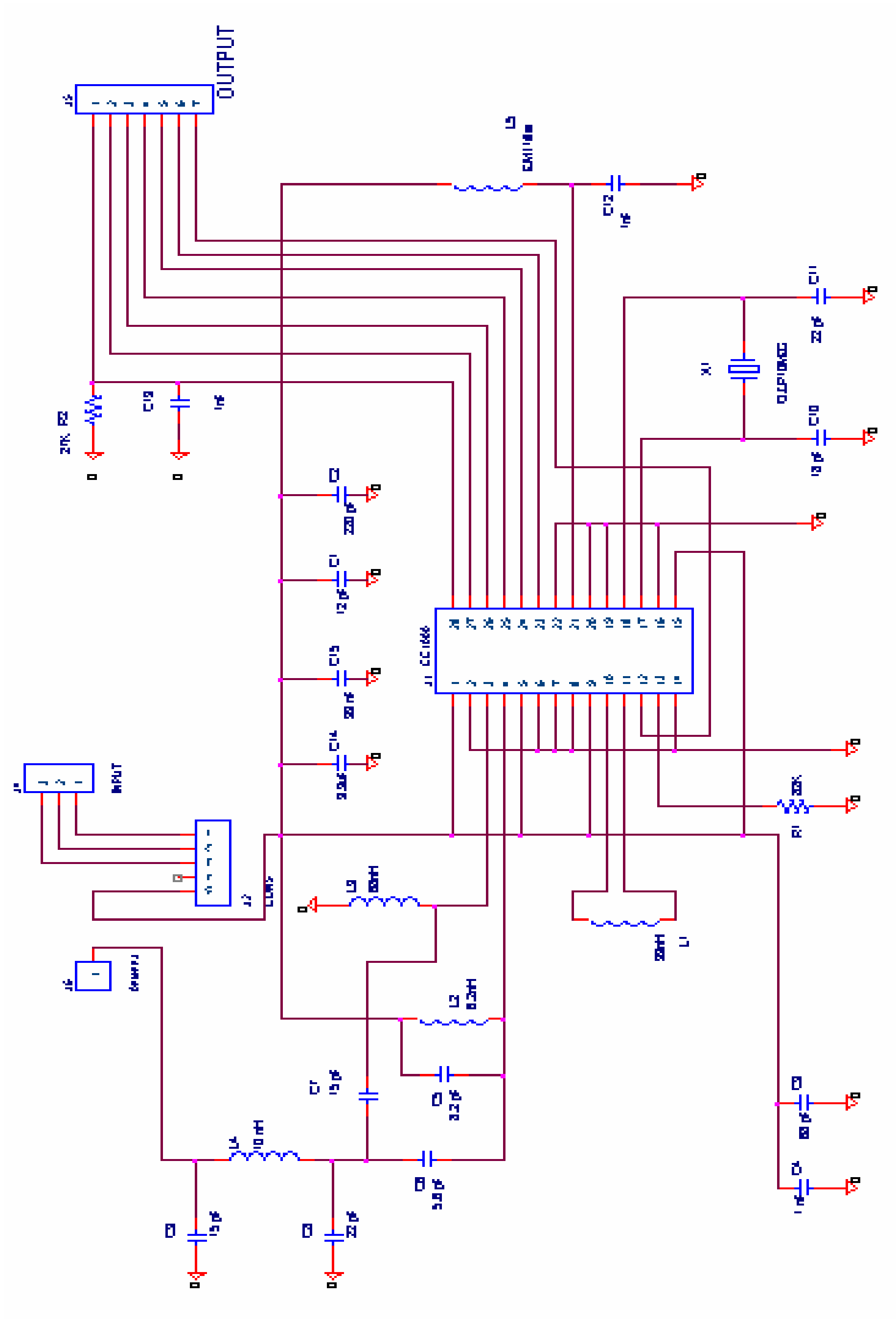

Figure 3: CC1000 circuit schematic

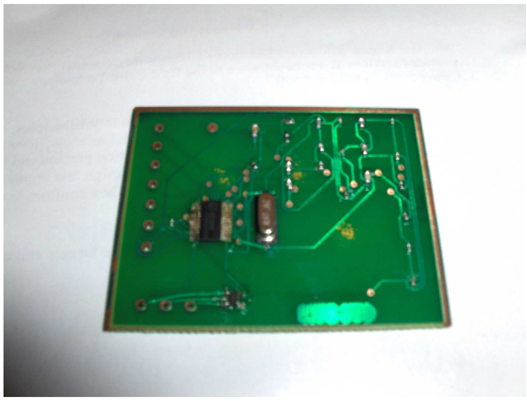

Figure 4: CC1000 circuit implementation

There were some problems during the implementation as there was a problem with very small passive component size which was not easily mounted on the PCB. Also the connection on the PCB needs to be done in an optimized way to minimize the losses as intrinsic capacitance affects RF circuits.

4.4. Tag implementation using 2.4GHz SPI Radio

In the second implementation the aim was not to spend time in the RF implementation and antenna design rather than concentrating upon the application itself. So a 2.4GHz SPI Radio with Integrated Print Antenna was used in this implementation. The following are the features of the RF module used:

- 2.4-GHz Direct Sequence Spread Spectrum (DSSS) complete radio module which includes integrated PCB Trace Antenna, and all external components
- Operates in the unlicensed worldwide Industrial, Scientific and Medical (ISM) band (2.400 GHz–2.483 GHz)
- 21mA operating current (Transmit @ –5 dBm)
- Transmit power up to +4 dBm
- Receive sensitivity up to –97 dBm
- Sleep Current <1 µA

- Operating range of up to 50m or more.
- DSSS data rates up to 250 kbps, GFSK data rate of 1 Mbps
- Separate 16-byte Transmit and Receive FIFOs
- Receive Signal Strength Indication (RSSI)
- Serial Peripheral Interface (SPI) control while in sleep mode
- 4-MHz SPI microcontroller interface
- Vertical or horizontal mounting
- Operating voltage from 2.4 to 3.6 volts
- Operating temperature from 0 to 70°C
- Size: 38.1 mm x 25.4 mm (1.5” x 1.0”)
- Weight: 27 grams

Atmega8L microcontroller was interfaced with this wireless module through Serial Peripheral Interface (SPI). The communication protocol has been implemented at the controller. The following is the Circuit schematic for the tag:

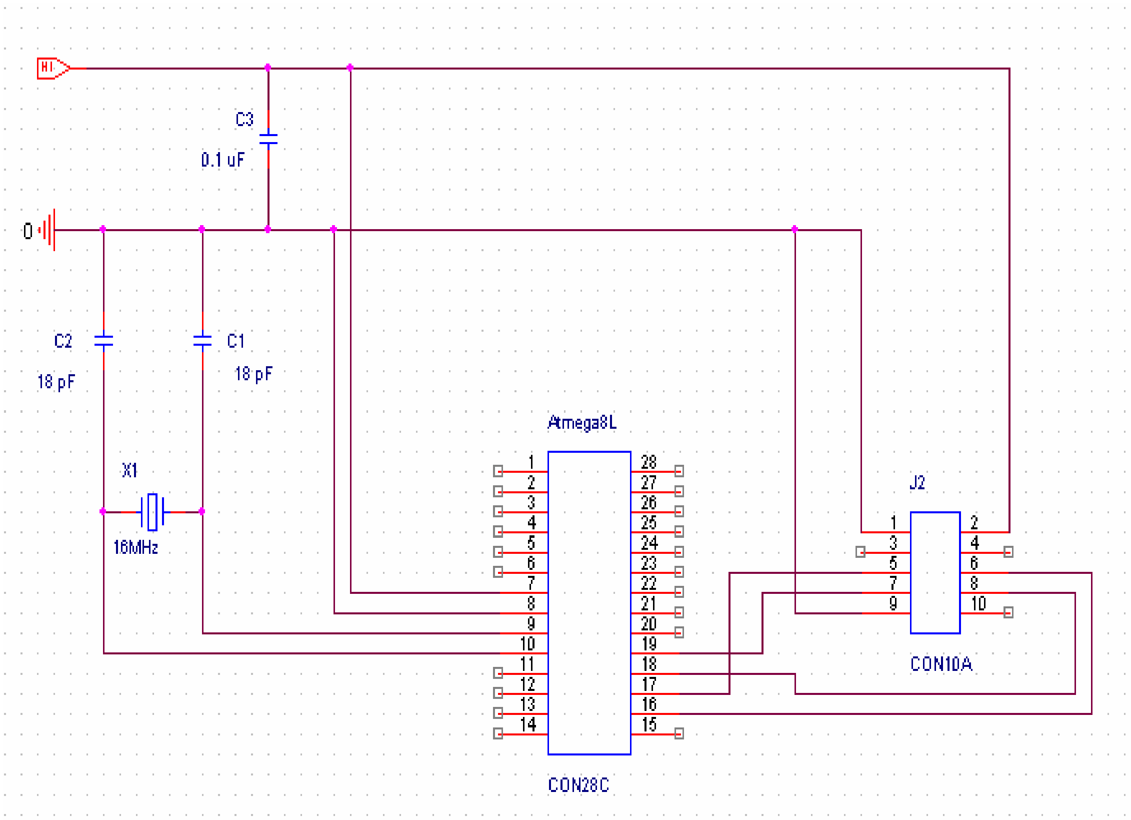

Figure 5: Vehicle's tag schematic

4.5. Cost of the vehicle's tag

The cost of the vehicle's tag is the most important factor affecting the cost of the whole system, as it will be deployed in every vehicle. Also it affects the feasibility of deploying the system, because as mentioned before, it will be required from the driver to buy this tag at the license renewal, so if the cost is relatively high, this will increase the public disapproval of the system.

The following is the cost of the vehicle's tag mentioned above [18]:

Table 3: Vehicle's tag cost

Part	Cost (USD)
2.4 GHz RF Module	5.6
Atmega8L Microcontroller	3
Battery	2
PCB	2
Other components	1.3
Total (USD)	**13.9 USD**
Total (EGP)	**77.84 EGP**

The above cost could be acceptable taking into consideration the cost of license renewal per year in Egypt.

4.6. Position of the tag in the vehicle

There are multiple positions where the EVI tag can be installed in the vehicle. According to the ISO standard ISO/DIS 24535 [22] for automatic vehicle identification the tag should be affixed to the front windscreen or embedded within the rear license plate of the vehicle. In our system, it is fixed to the windscreen to facilitate audio warnings, to avoid being damaged by a small car accident, and to allow an easy access to put a SIM card in case of toll collection. This position at the windscreen enables us to power the tag in the future with solar cells.

Chapter 5: Communication Protocol

In this chapter, at first we will present the some considerations in implementing the communication protocol between the vehicle's tag and the road-side reader. Based on these considerations the communication scheme is presented at the end of this chapter.

5.1. Communication protocol considerations

5.1.1. Data Integrity

The integrity of the data is the ability to differentiate between good Data and corrupted one, and this by adding some additional data (parity, checksum, CRC …etc) from which the validity of the original data is determined, also the ability to identify the error in the data received to be able to correct it or request for retransmission.

5.1.2. Data Security

The security of data is protecting the communication link from external attacks; these attacks could be as follows [23]:

- Unauthorized reading of a data carrier in order to duplicate and/or modify data.
- The placing of a foreign data carrier within the interrogation zone of a reader with the intention of receiving services without payment.

The security of data can be achieved via data encryption and mutual authentication

5.1.3. Collision avoidance

Avoiding collision in such a multi-access wireless field is the major parameter in both saving power and increasing the probability of reading the tags successfully which affects the efficiency of the overall system.

5.1.4. Minimum Overhead

For all above considerations, additional data is being added as an overhead to the original one to cover these requirements, but it must be taken into consideration also the coverage of these requirements with the minimum overhead for efficient utilization of the communication channel and the reduction of the node power consumption.

5.2. Data Integrity

Using wireless communication for data transfer is vulnerable to data corruption; this is due to multiple reasons like:

- Interference from other devices operating at the same frequency band, or data transmission from another vehicle’s tag.
- Multi-Path fading: This is due to radio signals reaching the receiving antenna by two or more paths. Effects of multi-path include constructive and destructive interference, and phase shifting of the signal. In digital radio communications multi-path can cause errors and affect the quality of communications. The errors are due to Inter-symbol interference (ISI).

So after the reception of the data, we need to check that this data is the same sent from the source, In general this is done through applying a certain calculation on the data before sending it from the source, and adding certain information which is the output of this calculation. On receiving the data this additional information is extracted and we make the same calculation on the original data, and compare the result with the additional data attached to check the consistency of the original one.

The type of calculation made should be selected carefully as this affects the probability of not detecting an Error and the ability of identifying the position of the error to be able to just request the re-transmission of the corrupted part or even correcting it without the need for re-transmission of the whole data packet, but there is a tradeoff between the capability of error detection and the data overhead.

The simplest form of error detection is the parity check. A parity check is accomplished by adding all of the '1's in a group of bits. For even parity, if the number is even, then the parity bit is set, otherwise it is not. For odd parity, if the number is odd, then the parity bit is set. The parity check is the easiest to implement, but is also the most unreliable. It can only catch an odd number of errors in the bit stream. If the number of errors is even, then the parity calculation will incorrectly indicate that the byte is good. Thus, there is 50% chance of the parity check catching an error.

Another technique which is calculating the checksum, a checksum is calculated based on a series of bytes by adding the values of the bytes together and truncating the result to the desired bit length of the overhead added data. A checksum will catch more errors than the parity check. However, by simply transposing data bytes 2 and 3 (for example), the data packet becomes corrupted, but the checksum would provide the same result. The checksum only gives weight to the value of the bytes, not their order. Thus, errors of ordering cannot be caught with the checksum.

The most popular form of error checking is the cyclic redundancy check (CRC). A CRC is more reliable than the checksum because every bit can individually contribute to the checksum. This makes it much less likely that multiple errors will cancel each other out. The mechanics of computing [24] an n-bit binary CRC are simple. The bits representing the input are lined up in a row, and the (n+1)-bit pattern representing the CRC's divisor (called a "polynomial") is positioned underneath the left-hand end of the row. Here is the first calculation for computing a 3-bit CRC:

```
11010011101100 <--- Input
1011           <--- divisor (4 Bits)
--------------
01100011101100 <--- result
```

If the input bit above the leftmost divisor bit is 0, do nothing and move the divisor to the right by one bit. If the input bit above the leftmost divisor bit is 1, the divisor is XORed into the input (in other words, the input bit above each 1-bit in the divisor is toggled). The divisor is then shifted one bit to the right, and the process is repeated until the divisor reaches the right-hand end of the input row. Here is the last calculation:

```
00000000001110 <--- result of multiplication calculation
00000000001011 <--- divisor (4 Bits)
--------------
00000000000101 <--- remainder (3 bits)
```

Since the leftmost divisor bit zeroed every input bit it touched, when this process ends the only bits in the input row that can be nonzero are the n bits at the right-hand end of the row. These n bits are the remainder of the division step, and will also be the value of the CRC function (unless the chosen CRC specification calls for some post processing).

The selection of generator polynomial is the most important part of implementing the CRC algorithm. The polynomial must be chosen to maximize the error detecting capabilities while minimizing overall collision probabilities.

The most important attribute of the polynomial is its length (the number of the highest nonzero coefficient), because of its direct influence of the length of the computed checksum.The most commonly used polynomial lengths are

- 9 bits (CRC-8)
- 17 bits (CRC-16)
- 33 bits (CRC-32)
- 65 bits (CRC-64)

When creating a new CRC polynomial or improving an existing CRC the general mathematical advice is to use an irreducible polynomial that satisfies all polynomical irreducibility constraints from modular arithmetics.

- Irreducibility in this case means that the polynomial cannot be divided by any polynomial except itself and 1 with zero remainder.
- Reducible polynomials can still be used, but their error correcting and detecting capabilities will be less effective. Some applications may choose to use reducible polynomials under certain conditions.

The properties of the generator polynomial can be derived from the algorithm definition

- CRCs with more than one nonzero coefficients are able to detect all single bit errors in the input message.
- CRCs can be used to detect all double bit errors in the input message shorter than 2k, where k is the length of the longest irreducible part of the polynomial.

- If the CRC polynomial is divided by x + 1 then no polynomial with odd number of nonzero coefficients can be divided by it. Hence, it can be used to detect odd number of errors in the input message (like single bit parity function).
- CRC polynomials detect (single) burst errors shorter than the number of the position of the highest polynomial coefficient.

5.3. Data Security

Exchanging Data over a Wireless Medium makes this Data at risk of external attacks; these attacks can be classified into [23]:

- Passive Attacks: Where the Attacker tries to listen into the transmission to discover confidential information for wrongful purposes.
- Active Attacks: Where the Attacker try to manipulate the transmitted data and alter it to his benefit.

We need perform mutual authentication to be sure that both the Vehicle's Tag and the Reader are authorized for Transferring data and to avoid duplicating the Data for wrongful Purposes like Duplicating the Transmission of Vehicle's Tag to Transmit a different ID or Duplicating the Reader Transmission for Accessing the Information of the Vehicles. After this Mutual Authentication, the Data being exchanged between the Vehicles' Tag and the Road-Side Reader need to be protected; this is done through encrypting the Data.

5.3.1. Mutual Authentication

Symmetric Key Mutual Authentication

For this type of Mutual Authentication, both the Reader and the Tag should be in possession of a secret Key. When the Tag Enters the Interrogation zone of the Reader, before they both starts to exchange information, the Reader First generates a Random Number *Ra* and sends *Ra'* which is the Encrypted Version of this number with an Algorithm Using the Secret Key as a parameter during the Encryption. The Reader send *Ra'* to the Tag, and when the Tag receives it, it uses its Key to Decrypt this number Back to *Ra* and in turn generates another Number *Rb* and Encrypts it also to *Rb',* then sends both *Ra* and *Rb'* back to the Reader. On receiving the *Ra* from the Tag, the Reader Checked the Validity of the Tag but remains to Validate him self to the Tag, so the Reader takes *Rb'* and Decrypts it back to *Rb* and send it to the Tag. On receiving *Rb* the tag also validated the Reader and they starts to exchange Data.

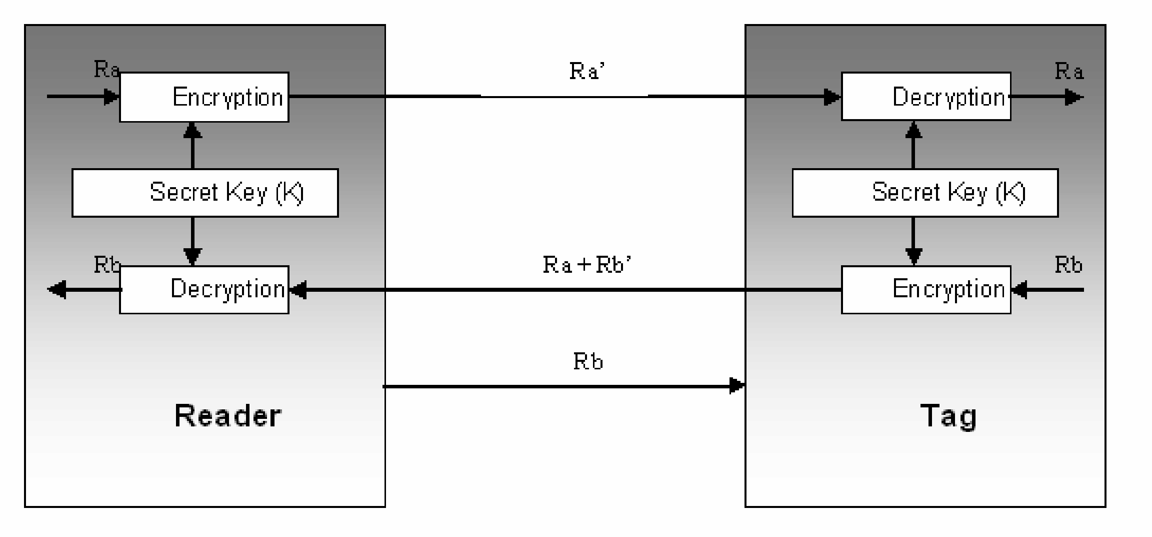

Figure 6: Symmetrical key mutual authentication

Derived Key Mutual Authentication

The Problem with the Symmetric Key is that both the Reader and Tag have the Same Key, so if this Key is compromised from one of the Tags, all the System will be Vulnerable to Attacks.

An Improvement can be done to the Authentication Procedure by assigning to each Tag a Different Key ***Kx*** while the Readers holds a Master Key ***Km***, from this Master Key and the ID of the Tag, each Tag's Key ***Kx*** Can be driven. So First the Reader Requests from the tag its ID, the Tag Replies with its ID along with a Generated Random Number *Ra* after Decrypting it with its Key ***Kx***, The Reader drives the Tag's Key ***Kx*** from the ID using its Master Key ***Km*** then uses this Key to Decrypt *Ra'*, Then a Random Numbe*r Rb* is Generated at the Reader and Encrypted using the Derived Key into *Rb'* and Sent Back to the Tag with *Ra*, the Tag then Decrypts *Rb'* and Replies to the Reader with *Rb* .

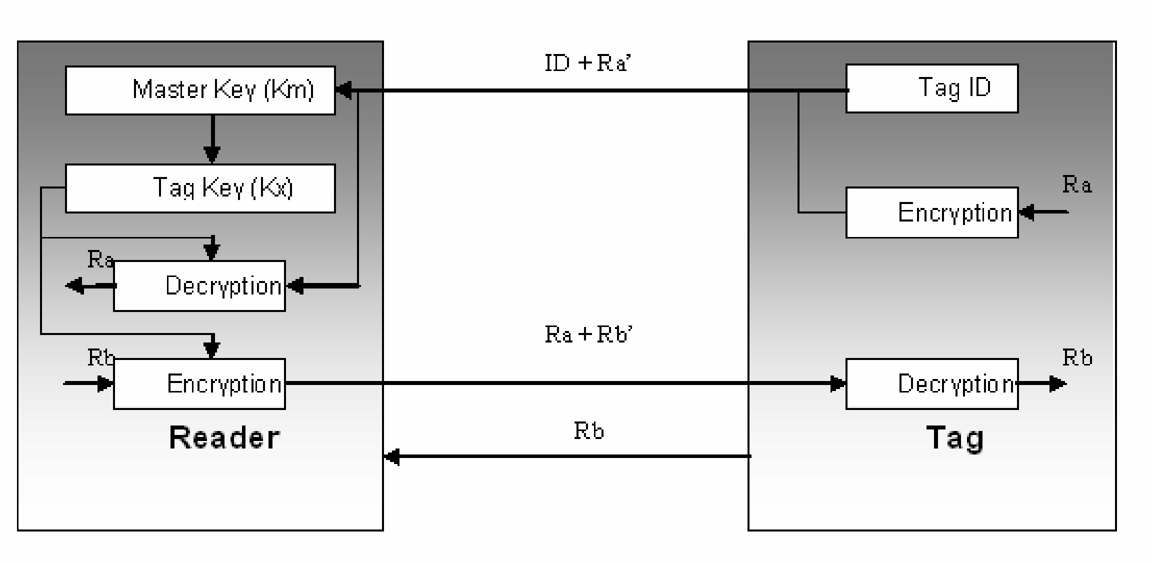

Figure 7: Derived key mutual authentication

5.3.2. Data Encryption

After the Mutual Authentication, the Data being exchanged between the Tag and the Reader need to be protected against Attackers who could Listen to the

Transmission of Data, So the Data should be Encrypted, this Encryption requires an Encryption algorithm in addition to a Key which is used by the Algorithm to convert the Transmitted Data into Cipher Data difficult to be Interpreted by any Attacker. This Cipher Data is decrypted at the Receiver.

If each character is individually encrypted prior to transmission, the procedure is known as sequential ciphering (or stream ciphering). If, on the other hand, several characters are incorporated into a block then this is called block cipher.

Stream Cipher

Sequential ciphers or stream ciphers are encryption algorithms in which the sequence of plain text characters is encrypted sequentially using a different function for every step.

The ideal realization of a stream cipher is the so-called *one-time pad*, also known as the *Vernam* cipher. In this procedure a random key K is generated, before the transmission of encrypted data, and this key is made available to both the Transmitter and the Receiver. The key sequence is linked with the plain text sequence by the addition of characters or using XOR gating. The random sequence used as a key must be at least as long as the message to be encrypted, because periodic repetitions of a typically short key in relation to the plain text would permit crypto-analysis and thus an attack on the transmission. Furthermore, the key may only be used once, which means that an extremely high level of security is required for the secure distribution of keys.

Stream ciphering in this form is completely impractical for RFID systems. To overcome the problem of key generation and distribution, systems have been created based upon the principle of the one-time pad stream cipher that uses a pseudorandom sequence instead of an actual random sequence. Pseudo random sequences are generated using pseudo random generators.

5.4. Collision Avoidance

Collision is one of the major problems encountered in multi-tag RFID systems. Detection\Avoidance of this collision is the key of having an efficient system. There are several algorithms used for collision avoidance.

Binary Search Algorithm:

In this algorithm each tag has a globally unique identifier (ID) represented by a string of bits. The reader is able to specify the range of tag IDs in the request message to which the tags coming under that range must respond with their IDs. In the first iteration, this ID is the maximum value possible of the group of IDs in the system. Then we calculate the binary step, which is the current ID divided by 2.

When the request is sent, if there is no response, we should add the binary step calculated before to the current ID and send another request (but the ID should be limited to the maximum possible ID in this addition operation).

If there was a response and there is a collision we should subtract the binary step from the current ID and send the request again. In the end if there is a successful response without collision, this ends the search by sending message exclusively to the tag which has been read successfully, while other tags does not respond to these messages.

Fig. 8 shows the flow chart which is executed at the reader applying binary search algorithm for reading multiple tag.

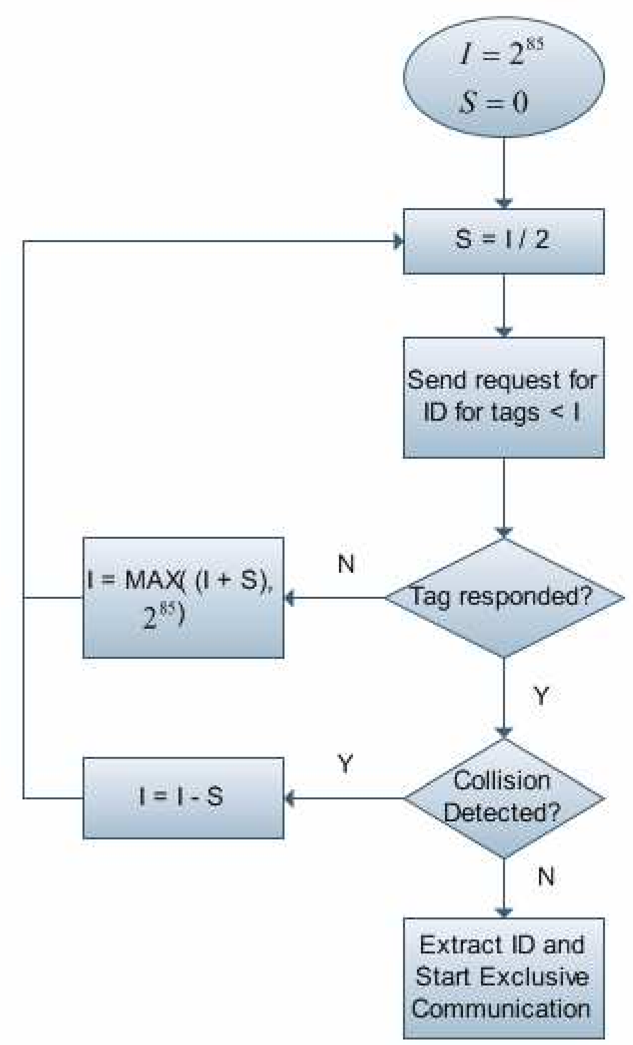
$I = 2^{85}$
$S = 0$
S = I / 2
Send request for ID for tags < I
Tag responded?
N
I = MAX((I + S), 2^{85})
Y
Collision Detected?
Y
I = I - S
N
Extract ID and Start Exclusive Communication

Figure 8: Binary search algorithm

‘I’ is the current ID during the search process.
‘S’ is the binary step.

Since the ID will be its VIN and the VIN consists of 17 characters, each character can be any of the numbers (1-9) and any other capital alphabetic letter except for the letters I, O or Q [25]. This requires 5 bits to represent each VIN character. So for the ID of the vehicle 85 bits are required.

‘I’ is initialized with 2^{85} which is the maximum VIN

The maximum number of iterations for establishing an exclusive communication with a single tag is $\lfloor \log_2(85) \rfloor = 7$ iterations

During the binary search the reader send the following packet:

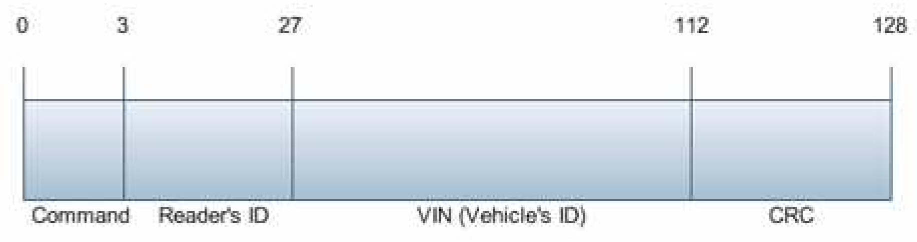

Figure 9: Packet format 1 (F1)

Command: 3 Bits from which the receiver of the packet identify the type of the packet. In case of binary search, this command will be 1 (binary: 001) when the reader send it, which will be interpreted by the tags as a request from all tags having an ID less than the VIN attached at the same packet to send back an acknowledge with there ID.

Reader's ID: 24 Bits for unique ID of the reader.

VIN: 85 Bits representing the Vehicle Identification Number (VIN).

CRC: 16 Bit Cyclic Redundancy Check

The same packet is also used by the vehicle's tag to identify itself during the binary search process, except that the command part will be with different value which will be 2 (binary: 010).

5.5. Communication Scheme

This section describes the communication scheme between the reader and the vehicle's tag.

After the binary search, the reader will clearly identify the vehicle which it will continue an exclusive communication session with. The next step is requesting the vehicle information, this through sending the same packet described at fig. 5.4 but with the command 3 (binary: 011) and the VIN is the one of the vehicle identified through the binary search.

All the vehicles in the zone covered by the reader will receive this packet. But reading the command '3' will make only the vehicle with the VIN specified at the packet replies to it. This vehicle replies with the same packet format in addition to its data:

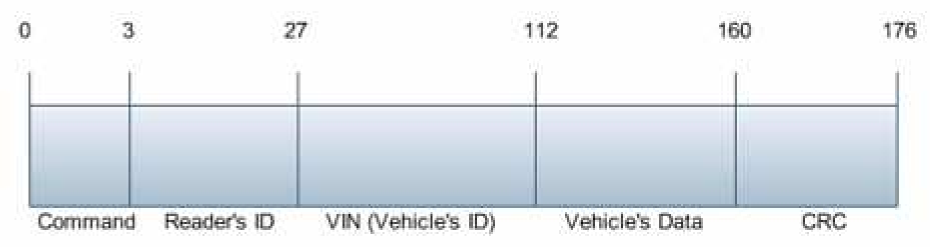

Figure 10: Packet format 2 (F2)

The above packet format is the same as the first one except for the vehicle's data which are 48 bits. These 48 bits are 8 bits which hold status flags. 1 bit used as warning flag indicating if the vehicle had a warning from a previous reader for exceeding the speed limit or not. Another bit indicating if the vehicle has a ticket or not. The remaining bits (6 bits) are reserved for quick future upgrades. Another 24 bits are for the last reader the tag succeeded to establish communication with. The last 16 bits represent the time since being identified at the last reader mentioned in the vehicle's data.

As mentioned in chapter 3, using the previous reader ID along with the time since that tag established communication to it, will be used by the current reader to calculate the speed of the vehicle through a calibration table stored in the reader with all the surrounding readers and their distances.

After receiving the vehicle's data the reader should process this data and reply back with the following packet:

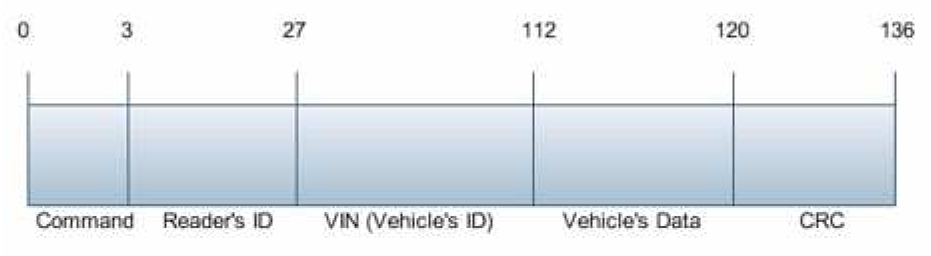

Figure 11: Packet format 3 (F3)

In this packet the command is 4 (binary: 100). The vehicle's data in this packet is just 8 bits which represents the group of flags updated by the reader. The tag replace the old data with this new one, while the previous reader ID is being replaced by the current one whose ID is included in the packet. After receiving this packet the tag should reset the timer to enable the next reader to calculate its speed like the current one

Finally the tag should reply to this packet to confirm updating its data. This is done through sending the packet format described before in figure 5.4, with the command 5 (binary: 101).

The following is the scheme described before:

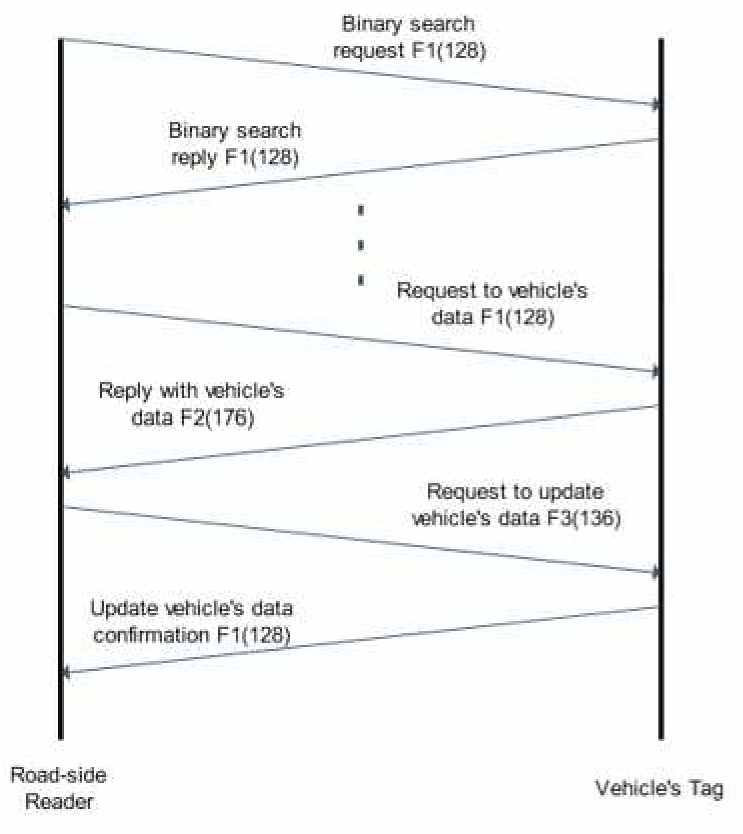
Binary search request F1(128)
Binary search reply F1(128)
Request to vehicle's data F1(128)
Reply with vehicle's data F2(176)
Request to update vehicle's data F3(136)
Update vehicle's data confirmation F1(128)
Road-side Reader
Vehicle's Tag

Figure 12: Communication scheme

After this confirmation, the communication session between this reader and this tag should end. The reader will start again its binary search for a new tag, during this search if the previous tag received a request from this reader to send its ID, the tag should ignore that request giving the opportunity to other tags to establish a communication session.

Chapter 6: System Evaluation and Verification

6.1. System time performance evaluation

In this section, the time performance of the system is evaluated. For evaluating the time performance, we need to calculate the time required for a single vehicle to be successfully detected by a road-side reader according to the protocol described earlier in chapter five.

There are three parameters affecting the time delay in this protocol:

- Time for the RF module to send the packet.
- Processing time in each of the vehicle's tag and the road-side reader.
- Propagation delay between the road-side reader and the vehicle's tag.

As mentioned in chapter four the RF module is operating in 250 kbps [26]. The processor of the Atmega8L is operating at 16 MIPS using 16MHz crystal [21]. For the calculation of the propagation delay we will assume worst case which is having the vehicle at maximum distance from the road-side reader which is 50ms [26] as mentioned before in chapter four.

For the following calculation we will assume the processing time at each step from the communication scheme to be 500 instructions on average (estimated from the assembly file of the software of both the reader and the tag).

So for the time sending each packet by the RF module (Ts), we will divide the number of bits being sent by the bit rate (250 kbps). For all the processing delay (Tp) at each step for both the road-side reader and the vehicle's tag, the time will be: Tp = 500 / (16 x10^6) = **0.03125ms.** For the propagation delay (Td), taking the case of 50m distance: Td = 50 / (3 x10^8) = **0.001666ms**

The following scheme is used to calculate the best case of detecting successfully a single vehicle by a road-side reader. In this case the binary search will end up by a single iteration:

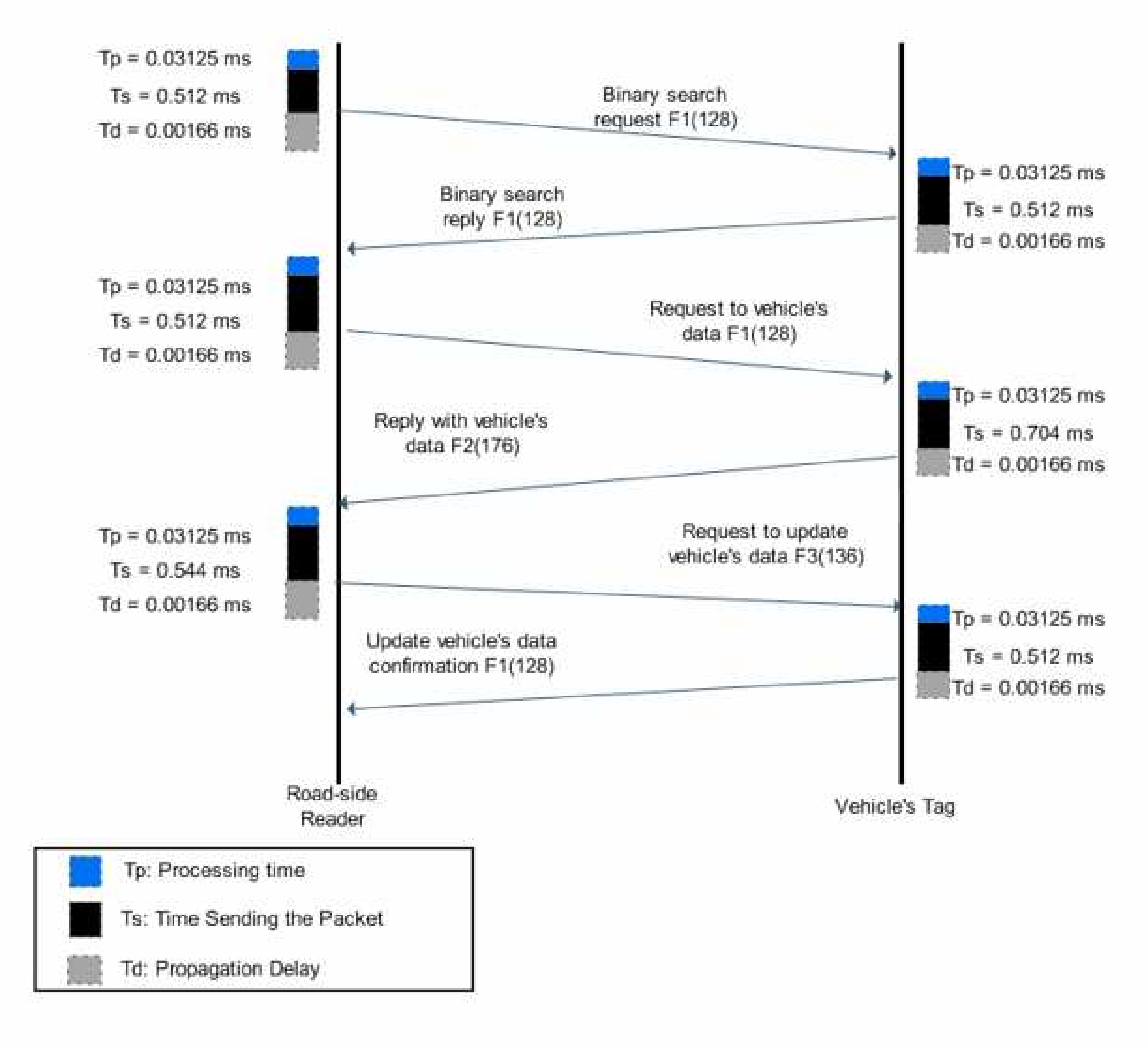

Figure 13: Communication scheme time analysis

From the above scheme the total time for establishing communication with a certain tag will be the summation of all the time delay factors at each step, which will be in this case: **3.4935 ms,** this is the best case scenario, having only one vehicle in the road-side reader zone at the time of sending the request.

For calculating the worst case scenario having multiple vehicles in the reading zone it will only differ in the binary search phase, which will be at the worst case done in seven iterations as calculated earlier in chapter five, so according to the communication scheme described in fig. 13, the time of additional six iterations will be added to the calculation. From the above scheme, a single iteration (sending binary search request and binary search reply) takes **1.0903 ms** so the total time for establishing communication with each vehicle in that case will be**:** 3.4935 + (6 x 1.0903) **= 10.0355 ms.**

Now that we have calculated the minimum and maximum time for establishing communication with each vehicle, we have to study if this time is sufficient for the road-side reader to detect a vehicle before exiting its reading zone. To do so we will consider a road-side reader covering a four lane road and four vehicles traveling at speed 200 km/hr going into the reading zone at the same time. We will assume that the length of each vehicle is 2.5 m, and then we will consider another four vehicles going into the reading zone just after the previous four vehicles as shown in fig. 14:

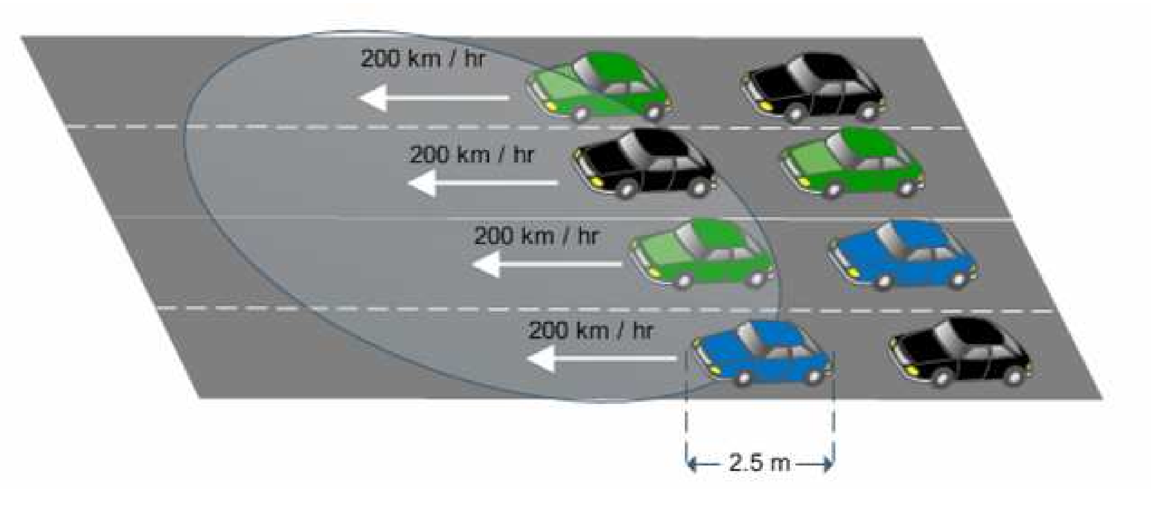

Figure 14: Road-side reader detecting vehicles

The worst case for detecting all the four vehicles is that three of these vehicles will take maximum iterations in the binary search phase while the fourth will take a single iteration in the binary search as the other vehicles will not reply to the reader's request. So in that case all four vehicles will establish communication with the reader in a time equals to: (3 x 10.0355) + 3.4945 = **33.601 ms**

In the previous scenario the duration before possibly having any another vehicle in the reading zone could be calculated by dividing the length of the vehicle (2.5m) by its speed (200 km/hr) which will be **45 ms.** This time is sufficient to establish communication with all four vehicles before any other vehicle enters the reading zone. Also this calculation is done assuming that there is no distance between these vehicles which is impossible in real life to having vehicles traveling at 200km/hr without any separating distance between them. But this case has been assumed to study the system in its worst case even if this case is theoretical.

6.2. Speed calculation error

In this section we calculate the error in calculating the speed of the vehicles and present the requirements for adjusting this error to an acceptable level.

The error in calculating the speed arises from being unable to identify exactly the position of the vehicle in the reading zone. And as mentioned before in chapter four, the reader covers a range of about 50m, and we will consider each successful reading to be done at exactly the position of the reader, this could make an error in the position of the by +/- 50m. And since the speed calculation also depends on the next reader, and the error in the position of the vehicle at that reader will be the same, so we will have +/- 100m error in the position of the vehicle in the speed calculation.

To minimize the effect of this error on the speed calculation, we need to increase the distance between two successive readers. But this distance should not be increased in a way that reduces one of the most important benefits of the system, which is being able to detect speed violation all along the roads.

A certain speed violation allowance is normally specified to avoid recording a speed violation ticket without the driver exceeding the speed limit, this allowance varies from one country to another, but normally it varies slightly around 10% of the speed limit [22]. So to achieve such an allowance in our system, the minimum required distance between two successive readers will be: 100m / 0.1 = **1 km**. Applying this distance as a minimum requirement along with 10% allowance in speed limit violations will avoid any error in the speed calculation.

6.3. Power performance evaluation

In our system, power consumption is one of the main concerns, especially the power of the vehicle's tag, as we need the vehicle's tag to operate for at least three years (maximum time before vehicle license renewal in Egypt) with a power source independent from the vehicle's battery.

From section 6.1, we deduced the time required to establish communication between vehicle's tag and road-side reader which was 33.601 ms traveling at speed 200km/hr. Also from the minimum requirement we deduced before in section 6.2 of having 1 km at least between each two readers, we deduce that the vehicle will not pass by another reader with that speed before 18 sec.

To calculate the power dissipated by the vehicle's tag we need to know for how long the vehicle's tag will be in each of the transmission, reception and sleep mode.

Having the ability to wakeup from the sleep mode on reception of a packet [27] we can make the vehicle's tag enters the sleep mode just after establishing communication with the reader. Which means that the vehicle's tag will be in sleep mode for: (18000 - 33.601 / 18000) * 100 % = **99.81332 %** of the time, while the rest of the time (0.18667 %) the tag will be in either transmitting or receiving mode to establish communication with the road-side reader.

From the communication scheme described earlier in section 6.1, assuming the worst case (seven iterations in the binary search phase) the vehicle will be transmitting 1200 bit while receiving 1160 bit, which means that during establishing communication with the road-side reader, the vehicle's tag will be in transmission mode for: (1200 / (1200 + 1160)) * 100 % = 50.84745 % of the communication time while receiving for: (100 - 50.84745) % = 49.15254 %.

Then the vehicle's tag will be in transmission mode for: (0.18667 * 50.84745) / (100) % = **0.09491 %** of the time, while receiving for: (0.1866722 * 49.15254) / (100) % = **0.09175 %** of the time.

According to the RF module datasheet [20] the following currents are required in each state:

- Sleep mode: 0.8μA.
- Tx mode: 26.2mA.
- Rx mode: 21.2 mA.

Also we need to consider the power dissipated in the microcontroller, the controller is also expected to be in active mode during both transmission and reception states and goes to sleep mode otherwise. The controller will be able to wakeup from the sleep mode upon receiving an interrupt from the RF module indicating a signal reception. According to the controller datasheet [28] the following currents are required in each state:

- Sleep mode : 0.5μA.
- Active mode : 3.6mA.

Then during 3 years (26280 hrs) the following power is required to be supplied by the battery:

- Sleep mode: (0.8µA + 0.5µA) * 26280 * (99.81332 / 100) = 34.10022 mAh.
- Tx mode : (26.2mA + 3.6mA) * 26280 * (0.09491 / 100) = 743.28197 mAh.
- Rx mode : (21.2mA + 3.6mA) * 26280 * (0.09175 / 100) = 597.97512 mAh.

Then for the vehicle's tag we need a battery of **1375.35731 mAh** to last for 3 years. Such a battery could be available in a small size (coin battery) with an appropriate cost (<2$) [18].

6.4. Other systems

6.4.1. CERT Falcon

CERT (Center of Excellence for applied Research and Training) in Dubai, in a partnership with IBM developed 'Falcon', a telematics technology platform that is able to support a wide variety of services for government authorities and private sector organizations. This system provides the following applications:

- Fleet management and tracking.
- Driver identification and driving behavior monitoring.
- Toll management.
- Automotive internet gateway.

The in-vehicle unit in this system has the following elements:

- GSM/GPRS module: used to communicate with the GSM network which in turn is connected to the command center through IP network, which also allows implementation of private applications (e.g. fleet management) through web-based applications.

- GPS module: used for vehicle's speed detection, navigation application and fleet management.
- CAN interface: used to connect to the vehicle's ECUs (Electronic Computing Units), to collect data about the vehicle (e.g. faults) to be sent.
- Audio Output: used to provide the driver with messages to avoid distraction during driving.

The in-vehicle unit is powered by the vehicle's battery. It should be installed inside the car for audio messages. It uses Freescale MPC5200 as a core processor, which costs about 22.8 USD [18], while the GPS - U-blox LEA-4S costs around 112 USD [18] in addition to Bluetooth module and a GPRS module.

- CERT Falcon VS. System presented:

Advantages:

- The CERT Falcon presents a wider range of applications than our system, in addition to more flexibility to extend its applications due to multiple communication interfaces.

Disadvantages:

- The on-board unit of CERT Falcon is much more expensive (>130 $) than that presented in our system due to multiple communication modules and consequently a powerful processor to handle them.
- The CERT Falcon requires to be connected to car battery as it consumes large power (3W) [29]. This makes the installation more difficult and increases the possibility of tampering.

6.4.2. E-Plate

This project is developed by IDENTEC SOLUTIONS, the plates are the same size and shape of the conventional plates but each plate contains an embedded active RFID tag operating at 868MHz or 915 MHz, these tags are battery operated. Each tag continuously (each 500ms) sends a unique encrypted identification No. and can be detected by readers from a distance up to 100 meters [30].

The ID broadcast of the tag is detected by roadside readers which are connected to the control center for data processing.

Applications:

- Electronic toll collection.
- Vehicle anti-theft check.

- E-Plate VS. System presented:

Advantages:

- Longer battery life time (10 years).
- Cost of the on-board unit could be less, as the communication between the reader and the tag is one-way communication.

Disadvantages:

- Providing limited applications due to one-way communication between the tag and the reader. Currently the system doesn't support speed limitation application as in that case synchronization between all readers will be required in addition to being unable to give the driver a warning like in our system.
- Connecting the tag to the rear license plate makes it more vulnerable to damage by simple car accidents.

Table 4: Systems' comparison

	System Presented	CERT Falcon	E-Plate
Applications	●● Speed limitations. ETC.	●●●● Fleet Tracking. Driver Behavior Monitoring. Vehicle Internet Gateway.	● ETC Anti-Theft
Cost (On-board unit)	●● ~14 $	●●●● >130$	● N/A
Cost (Running cost)	●● Maintenance	●●● Maintenance + GPRS usage	●● Maintenance
Battery Life time	● (>3 years)	●●●● (N/A: connected to vehicle's battery)	●● ~ 10 years

Chapter 7: Conclusion and Future Trends

7.1. Conclusion

Contribution of information technology in the transportation sector helps in improving the efficiency and safety of such an important sector. In this thesis we presented an EVI system which provides two useful applications: speed limitation and electronic toll collection.

Speed limitation application in EVI system helps in detecting the speed of vehicles inside the city and on highways without affecting the traffic flow, which reduces the number of accidents, knowing that the speed of the vehicle is detected most of the time.

The electronic toll collection application debits the accounts of registered vehicles without requiring them to stop. Such an application improves the efficiency of the utilization of the transportation infra-structure. Also this allows the application of dynamic fees on main routes inside the city which could vary along a single day, so that these fees are at maximum during rush hour for example. Hence, it is possible to tune the traffic flow over the day with such a non-blocking technique.

We reviewed the technologies commonly used to implement this system like RFID, DSRC, GSM and Bluetooth, and then according to technical considerations (power consumption, data rate and operating range) and non-technical considerations (cost, road-infra-structure and installation) we chose active RFID technology to implement our EVI system due to its low power consumption, relative long range (~50 m), low cost and an appropriate data rate to our target applications.

We presented the system structure, which consists of three main components: vehicle's tag, road-side reader and traffic control center.

One of the major problems for deploying the system is the lack of communication and electrical infra-structure in most of the highway roads in Egypt, which makes it difficult to establish a connection between the road-side reader and the traffic control center. So the system operation was designed to overcome this problem by using the vehicles to forward messages between the readers, till the message reaches a reader connected to the traffic control center, this way only few road-side readers could be connected to the control center reducing the cost of deploying the system.

A prototype of the vehicle's tag and the road-side reader was implemented. We presented the details for the hardware implementation, having a 2.4 GHz RF module as the communication module connected to a controller through Serial Peripheral Interface (SPI).

Also the cost of the vehicle's tag was calculated and it was about 14 US $, this value is an appropriate value to be requested from each driver to pay at license renewal.

We also presented the communication protocol between the vehicle's tag and the road-side reader. There was a challenge for the reader to establish communication with all the vehicles in the reading zone especially that the vehicles are in motion and the time is limited before leaving the reading zone. Binary search algorithm was used by the reader to avoid collision, and by analyzing the usage of the search algorithm in our system we concluded that the maximum search iterations before detecting a vehicle is seven iterations.

After detecting a single vehicle's tag, the reader starts an exclusive communication session with the vehicle's tag to extract its information, the details of the communication scheme was presented with each frame format.

We evaluated the time performance of the system by calculating the time required for the reader to detect vehicles before leaving its reading zone. We took the worst case of having a group of vehicles aligned and moving at speed 200km/hr into the reading zone, and calculated the time required for the reader to establish communication with all of them according to the communication scheme designed. The time at maximum was 33.601 ms while the time for having new group of vehicles entering the reading zone is 45 ms, so the system proved to be successful and scalable in terms of time performance.

We evaluated the system also for the power performance, and calculated the power required by the vehicle's tag in three years, which is the maximum time in Egypt before license renewal, and this to be able to replace the battery by the traffic authority at that time. The power required was 1375.3 mAh which is possible to be supplied by coin battery with the cost estimated.

In any speed detecting approach, there should be a margin left to compensate the error in the calculation, this speed violation allowance is normally specified to avoid recording a speed violation ticket without the driver exceeding the speed limit. We calculated this error in our system and derived a requirement of having 1km minimum spacing between two successive readers to limit this allowance to 10%.

Finally we compared our system to other systems like CERT falcon in Dubai and E-plate in the UK, taking into consideration the cost against the applications provided and our system showed providing very useful applications with an appropriate cost.

7.2. Future Trends

The thesis opens the door to the following field of research:

- Design and implement the communication scheme between the road-side reader and the communication center.
- Collecting real time data about the traffic state and using the vehicle's to forward this data to the traffic control center. This could lead to better utilization of the transportation infra-structure.

- Navigation application to the system, by providing the directions to the driver reaching his destination, according to real time data about the traffic.
- Ambulance alarm application on EVI system which allows the ambulance to communicate directly with the vehicle's on the road giving them a warning to clear the way.
- Adding collision warning application which allows communication between vehicles and warn the driver about any possible collision.
- Using bar code technology for detecting the vehicles in EVI system [31], which could be a better option in terms of the cost of the vehicle's tag. Although it could provide limited applications due to the lake of a two-way communication.
- Establishing vehicle to vehicle communication to forward useful messages about the traffic [33].

REFERENCES

1. Jun-Wei Hsieh, Shih-Hao Yu, Yung-Sheng Chen, and Wen-Fong Hu. “Automatic Traffic Surveillance System for Vehicle Tracking and Classification”. IEEE Transactions on intelligent transportation system, June 2006.

2. Alan Stevens and Brian Stoneman. “Electronic vehicle identification for road traffic information and enforcement”. Road Transportation and Information Control 11th Conference, 2002.

3. The world health report 2002 – Reducing Risks, Promoting Healthy Life - www.who.int/whr/2002/en/

4. R. Want. “An Introduction to RFID Technology”. IEEE Pervasive Computing, vol. 5, no. 1, pp. 25-33, January-March 2006.

5. Mojix Redefines the Range for Passive RFID - www.rfidradio.com.

6. Phil Blythe. “RFID For road tolling, road-use pricing and vehicle access control”. IEEE Transactions on wireless of communication, 1999.

7. Jack Opiola and Booz Allen Hamilton. “Vehicle Infrastructure Integration (VII) in the US - Enhancing Safety,Enabling Mobility”.IEEE Transactions on intelligent transportation system, 2006.

8. Hyunseo Oh, Chungil Yae, Donghyon Ahn and Hanberg Cho. “5.8 GHz DSRC Packet Communication System for ITS Services”. ITSS conference, 1999.

9. Khali Persad, C. Michael Walton and Shahriyar Hussain. “Electronic Vehicle Identification: Industry Standads, Performance, and Privacy Issues. Vehicle/License Plate Identification for Toll Collection Applications conference, January 2006.

10. Richard Wolff. "DSRC: A short range wireless technology for Telematics Applications", IEEE Transactions on intelligent transportation system, 2004.

11. Daniel Jiang, Vikas Taliwal, Andreas Meier and Wieland Holfelder. “Design of 5.9 GHz DSRC-based vehicular safety communication”. IEEE Transactions on wireless of communication, October 2006.

12. Bluetooth technical standards - http://www.bluetooth.com.

13. Global System for Mobile - http://www.gsmworld.com.

14. Bin Li, Xiaojing Wang, Hua Cai and Chunyan Wang. “The R&D Strategy for Intelligent Highway System of China”. IEEE Transactions on intelligent transportation system, 2003.

15. Jinhua Guo and Nathan Balon. “Vehicular Ad Hoc Networks and Dedicated Short-Range Communicaion”. University of Michigan publication, June 2006.

16. H. Cai, Y. Lin. “Design of a roadside seamless wireless communication system for intelligent highway”. IEEE, Intelligent Transportation System. 2005

17. Jinhua Guo.“Vehicle Safety Communications in DSRC”. IEEE, Intelligent Transportation System, 2006.

18. Digi-Key electronic parts supplier catalog - www.digikey.com.

19. GSM World: Egypt’s coverage map - www.gsmworld.com/roaming/gsminfo/cou_eg.shtml.

20. National Telecommunication Regulatory Authority – Egyptian radio spectrum allocation chart.

21. International Telecommunication Union - http://www.itu.int/publ/R-REG-RR/

22. Intelligent transport systems — Automatic vehicle identification — Basic electronic registration identification (Basic ERI) - INTERNATIONAL STANDARD ISO/DIS 24535.

23. Klaus Finkenzeller. “RFID Handbook - Fundamentals and Applications in Contactless Smart Cards and Identification”. Second Edition 2002.

24. Peterson, W. W. and Brown, D. T. "Cyclic Codes for Error Detection". Proceedings of the IRE 49: 228, January 1961.

25. United States Federal VIN Requirements (Title 49, Chapter V, Part 565) - http://www.access.gpo.gov.

26. Cypress Semiconductors official website, CYRF6936 – Datasheet: www.cypress.com/

27. Atmel official web site, Atmega8L Datasheet: www.atmel.com/dyn/products/datasheets

28. European Road Safety Observatory "http://www.erso.eu/"

29. CERT Infotrack Telematics – CERT Falcon system overview - http://www.certinfotrack.com/

30. E-plate official website: www.e-plate.com.

31. Myung-Ryul Choi, 'Jin-Sung Park, Sang-Sun Lee. Seung-Ho Tak, "Automatic Vehicle-Identification System", IEEE Transactions on intelligent transportation system, 1996.

32. Hermann Rohling and Holger Busche, "Self-Organizing Traffic Information System based on Inter-Vehicle Communications", International workshop on intelligent transportation system (WIT), 2009.

APPENDICES

APPENDIX A: Road-side Reader Binary Search Code

```
#include <Atmega8L.h>
#include <Types.h>
#include <SPI_DRV.h>
#include <SysInit.h>
#include <lpradio.h>
#include <EVI.h>
#include <BinaryDetection.h>

#define RESPONSE_TIME_OUT 65535
#define COLLISION_TIME_OUT 65535

void StartDetection(void)
{
   u8  bVehicleDetected;
   u8  u8RxLength, u8LoopIndex,
        u8ArraySize, u8OldArraySize,
        u8BinarySearchStep, u8NewSmallDiffID, u8OldSmallDiffID,
u8RadioStatus,
        u8BinarySmallStep;
   u16  u16ResponseTimeOut, u16CollisionTimeOut;

   /*Initilization*/

   u8ArraySize = 8;
   u8OldArraySize = 0;
   u8BinarySearchStep = 4;
   u8NewSmallDiffID = 8;
   u8OldSmallDiffID = 0;
   bVehicleDetected = 0;
   u16ResponseTimeOut = 0;
   //
   u8TxPacket[1] = (u8)(u32ReaderID & 0x000000FF);
   u8TxPacket[2] =  (u8)((u32ReaderID & 0x000000FF)>>8);
   u8TxPacket[3] = (u8)((u32ReaderID & 0x000000FF)>>16);

      //All Send Command
   while(bVehicleDetected == 0)
   {
      if(u16ResponseTimeOut == 0)
      {
         u8TxPacket[0] = 0x01;
         for (u8LoopIndex = 4; u8LoopIndex < 15; u8LoopIndex++)
         {
            u8TxPacket[u8LoopIndex] = 0xFF;
         }
         RadioStartTransmit(u8TxPacket, 14);
         u16ResponseTimeOut = RESPONSE_TIME_OUT;
      }
      else
      {
         RadioStartReceive();
         u8RadioStatus = RadioRead(RX_IRQ_STATUS_ADR);
         //**Response
         if (u8RadioStatus & RXC_IRQ)
         {
            if((u8RadioStatus & RXE_IRQ) && (u16CollisionTimeOut != 0))
            {
               u16CollisionTimeOut --;
            }
            //** Collision
            else if (u16CollisionTimeOut == 0)
            {
               //Init ResponseTimeout
               while(bVehicleDetected == 0)
               {
                  if((u16ResponseTimeOut == 0) || (u16CollisionTimeOut
== 0))
                  {
                     u8TxPacket[20] = 0;
                     //Send less than
                     u8TxPacket[0] = 0x01;
                     for(u8LoopIndex = 1; u8LoopIndex <= u8ArraySize;
u8LoopIndex++)
                     {
                        u8TxPacket[u8LoopIndex] = 0xFF;
                     }
                     if(u8BinarySearchStep == 0)
                     {
                        u8TxPacket[u8ArraySize] =
(u8TxPacket[u8ArraySize] >> (8 - u8BinarySmallStep));
                     }
                     RadioStartTransmit(u8TxPacket, 14);
                     u16ResponseTimeOut = RESPONSE_TIME_OUT;
                     u16CollisionTimeOut = COLLISION_TIME_OUT;
                  }
                  else
                  {
                     RadioStartReceive();
                     u8RadioStatus = RadioRead(RX_IRQ_STATUS_ADR);
                     if (u8RadioStatus & RXC_IRQ)
                     {
                     //**Response
                        if((u8RadioStatus & RXE_IRQ) &&
(u16CollisionTimeOut != 0))
                        {
                           u16CollisionTimeOut --;
                           //**Collision
                           if(u16CollisionTimeOut == 0)
                           {
                              u8OldArraySize = u8ArraySize;
                              u8ArraySize = u8ArraySize -
u8BinarySearchStep;
                              u8BinarySearchStep = (u8)((u8OldArraySize
- u8ArraySize) / 2);
                              if (u8BinarySearchStep == 0)
                              {
                                 u8OldSmallDiffID = u8NewSmallDiffID;
                                 u8NewSmallDiffID = u8NewSmallDiffID - 
u8BinarySmallStep;
                                 //Next Small Binary Step
                                 u8BinarySmallStep = 
(u8)((u8OldSmallDiffID - u8NewSmallDiffID) / 2);
                              }
                           }
                        }
                        else
                        {
                           //Extract ID and Start Communication
                           u8RxLength = RadioRead( RX_COUNT_ADR );
                           RadioSlaveSelect();
                           RadioTransferByte(RX_BUFFER_ADR);
                           for (u8LoopIndex = 0; u8LoopIndex < 
u8RxLength; u8LoopIndex++)
                           {
                              RadioTransferByte(0xFF);   //Dummy Data
                              u8RxPacket[u8LoopIndex] = SPDR;
                           }
                           RadioSlaveRelease();
                           bVehicleDetected = 1;
                        }
                     }
                     else
                     {
                        u16ResponseTimeOut --;
                        //**No Response
                        if (u16ResponseTimeOut == 0)
                        {
                           //Load ID (Array + (Array/2)) Elements with 
0xFF
                           u8OldArraySize = u8ArraySize;
                           u8ArraySize = u8ArraySize + 
u8BinarySearchStep;
                           //Next Binary Step
                           u8BinarySearchStep = (u8)((u8ArraySize - 
u8OldArraySize) / 2);
                           //If the Difference Between the Tags is in 
the same Byte
                           if (u8BinarySearchStep == 0)
                           {
                              u8OldSmallDiffID = u8NewSmallDiffID;
                              u8NewSmallDiffID = u8NewSmallDiffID + 
u8BinarySmallStep;
                              //Next Small Binary Step
                              u8BinarySmallStep = 
(u8)((u8NewSmallDiffID - u8OldSmallDiffID) / 2);
                              //If the Vehicle Setection missed
                              if(u8BinarySmallStep == 0)
                              {
                                 //To start from the begining
                                 u16ResponseTimeOut = 0;
                              }
                           }
                        }
                     }

                  }
               }
            }
            // **No Collision
            else
            {
               //Extract ID and Start Communication
               u8RxLength = RadioRead( RX_COUNT_ADR );
               RadioSlaveSelect();
               RadioTransferByte(RX_BUFFER_ADR);
               for (u8LoopIndex = 0; u8LoopIndex < u8RxLength;
u8LoopIndex++)
               {
                  RadioTransferByte(0xFF);   //Dummy Data
                  u8RxPacket[u8LoopIndex] = SPDR;
               }
               RadioSlaveRelease();
               bVehicleDetected = 1;
            }
         }
         // No Response
         else
         {
            u16ResponseTimeOut --;
         }
      }
   }
   //**No Response => Start Again --
}
```

APPENDIX B: Road-side Reader Communication Code

```
#include <Atmega8L.h>
#include <Types.h>
#include <SPI_DRV.h>
#include <SysInit.h>
#include <lpradio.h>
#include <BinaryDetection.h>
#include <Reader_Config.h>

u8 u8TxPacket[21], u8RxPacket[21];
u16 u16TimeDuration;
u32 u32PreviousReaderID, u32PrevReaderDistance, u32VehicleSpeed;

void main(void)
{
   u8 u8LoopIndex;
   u8 u8RadioStatus;
   u8 u8RxLength;
   // Initialize the system
   SysInit();
   // Initialize the SPI
   SPI_MasterInit();
   RadioInit( (ACK_EN | END_STATE_IDLE | ACK_TO_12X), (TX_CFG_RST |
DATMODE_328DR) );
   RadioSetChannel( 2 );

   while(1)
   {
      //Init
      u32PreviousReaderID = 0;
      u32PrevReaderDistance = 0;
      u32VehicleSpeed = 0;
      StartDetection();

      //Request to send Info.
      u8TxPacket[0] = 0x03;
      u8TxPacket[1] = (u8)(u32ReaderID & 0x000000FF);
      u8TxPacket[2] = (u8)((u32ReaderID & 0x000000FF)>>8);
      u8TxPacket[3] = (u8)((u32ReaderID & 0x000000FF)>>16);
      for(u8LoopIndex = 4; u8LoopIndex < 15; u8LoopIndex++)
      {
         u8TxPacket[u8LoopIndex]  =   u8RxPacket[u8LoopIndex];
      }
      RadioStartTransmit(u8TxPacket, 14);

      //Begine Listening
      RadioStartReceive();
      do
      {
            u8RadioStatus = RadioRead(RX_IRQ_STATUS_ADR);
      }while((u8RadioStatus & RXC_IRQ) == 0);

      //Receive Info.
      u8RxLength = RadioRead( RX_COUNT_ADR );
      RadioSlaveSelect();
      RadioTransferByte(RX_BUFFER_ADR);
      for (u8LoopIndex = 0; u8LoopIndex < u8RxLength; u8LoopIndex++)
      {
                  RadioTransferByte(0xFF);
                  u8RxPacket [u8LoopIndex] = (SPDR ^ 0xFF);
      }
      RadioSlaveRelease();
      // Speed Calculation
      u32PreviousReaderID =(u32) ((u32)u8RxPacket[15]  | (
((u32)u8RxPacket[16]  << 8)) | (((u32)u8RxPacket[17]  << 16)));
      u32PrevReaderDistance = 0;
      for (u8LoopIndex = 0; u8LoopIndex < u8ReaderTableSize;
u8LoopIndex++)
      {
            if(ReadersTable[u8LoopIndex].ID == u32PreviousReaderID)
            {
                  u32PrevReaderDistance =
ReadersTable[u8LoopIndex].Distance;
            }
      }
      if(u32PrevReaderDistance != 0)
      {
            u16TimeDuration =  (u16)(u8RxPacket[18]  |
((u16)u8RxPacket[19]  << 8));
            //Resolution of Speed = (500000/2^32) / 0.1 =  0.001164
m/sec
            u32VehicleSpeed = u32PrevReaderDistance / u16TimeDuration;
      }
      //If Speed Limit Violation
      if (u32VehicleSpeed >= u32ZoneSpeedLimit)
      {
            // if there is a previous warning
            if((u8RxPacket[20] & 0x01) == 1)
            {
            // Raise Ticket Flag
            u8RxPacket[20] |= 0x20;
            }
            //No Warning before
            else
            {
            //Raise Warning Flag
            u8RxPacket[20] |= 0x01;
            }
      }
      // No Speed Limit Violation
      else
      {
            // Do nothing
      }

      //Request to Update Info.
      u8TxPacket[0] = 0x06;
      u8TxPacket[1] = (u8)(u32ReaderID & 0x000000FF);
      u8TxPacket[2] = (u8)((u32ReaderID & 0x000000FF)>>8);
      u8TxPacket[3] = (u8)((u32ReaderID & 0x000000FF)>>16);
      RadioSlaveSelect();
```

```
        RadioStartTransmit(u8TxPacket, 20);
    }
}
```

APPENDIX C: Vehicle’s Tag Communication Code

```
#include <Atmega8L.h>
#include <Types.h>
#include <SPI_DRV.h>
#include <SysInit.h>
#include <lpradio.h>
#include <EVI.h>


void main(void)
{
   u8 RxData [16] = {0};
   u8 RxLength;
   u8 RadioStatus;
   u8 LoopIndex;

   SysInit();
   SPI_MasterInit();
   RadioInit( (ACK_EN | END_STATE_RXSYNTH | ACK_TO_12X), (TX_CFG_RST |
DATMODE_328DR) );
   RadioSetChannel( 2 );
   PORTC = 0xFF;
   RadioWrite(XACT_CFG_ADR, END_STATE_RX);

   while (1)
   {
      RadioStartReceive();
      RadioStatus = RadioRead (RX_IRQ_STATUS_ADR);
      if (RadioStatus & RXC_IRQ)
      {
        if ( RadioStatus & RXE_IRQ )
      // If we had a buffer error...
         {
            lpRadioEmptyFile( RX_BUFFER_ADR, RxLength );
            PORTC =  0x33;
         }
         else
         {
            RxLength = RadioRead( RX_COUNT_ADR );
            RadioSlaveSelect();
            RadioTransferByte(RX_BUFFER_ADR);
            for (LoopIndex = 0; LoopIndex < 16; LoopIndex++)
            {
                  RadioTransferByte(0xFF);
                  RxData [LoopIndex] = (SPDR ^ 0xFF);
            }
            RadioSlaveRelease();
            //Check the command bits
            switch((RxData[0] & 0x07))
            {
            //Request to send ID
            case(0x01)
               u32CurrentReaderID = 0 | (RxData[0] & 0xF8) |
                                        (RxData[1] & 0xFF) |
                                        (RxData[2] & 0xFF) |
                                        (RxData[3] & 0x03);
               if(u32CurrentReaderID != u32PreviousReaderID)
               {
                  //Send Vehicle ID
                  u8TxPacket[0] = 0 | 0x02 | u32VehicleIDLowC;
                  u8TxPacket[1] = (u8)(u32VehicleIDM & 0x000000FF);
                  u8TxPacket[2] = (u8)((u32VehicleID & 0x000000FF)>>8);
                  u8TxPacket[3] = (u8)((u32VehicleID &
0x000000FF)>>16);
                  RadioSlaveSelect();
                  RadioStartTransmit(u8TxPacket, 20);
               }
            break;

            //Request to Send Vehicle's Info
            case(0x03)
               u32CurrentReaderID = 0 | (RxData[0] & 0xF8) |
                                        (RxData[1] & 0xFF) |
                                        (RxData[2] & 0xFF) |
                                        (RxData[3] & 0x03);
               if(u32CurrentReaderID != u32PreviousReaderID)
               {
                  u8TxPacket[0] = 0 | 0x02 | u32VehicleIDLowC;
                  u8TxPacket[1] = (u8)(u32VehicleIDM & 0x000000FF);
                  u8TxPacket[2] = (u8)((u32VehicleID & 0x000000FF)>>8);
                  u8TxPacket[3] = (u8)((u32VehicleID &
0x000000FF)>>16);
                  u8TxPacket[4] = (u8)(u32PreviousReaderID &
0x000000FF);
                  u8TxPacket[5] = (u8)((u32PreviousReaderID &
0x000000FF)>>8);
                  u8TxPacket[6] = u8VehcileData;
                  RadioStartTransmit(u8TxPacket, 20);
               }
            break;

            //Request to Update Info.
            case(0x05)
               u32CurrentReaderID = 0 | (RxData[0] & 0xF8) |
                                        (RxData[1] & 0xFF) |
                                        (RxData[2] & 0xFF) |
                                        (RxData[3] & 0x03);
               if(u32CurrentReaderID != u32PreviousReaderID)
               {
                  //updating vehicle's data (Ticket flag, warning flag)
                  u8VehcileData = RxData[13];
                  //send the acknowledge
                  u8TxPacket[0] = 0 | 0x02 | u32VehicleIDLowC;
                  u8TxPacket[1] = (u8)(u32VehicleIDM & 0x000000FF);
                  u8TxPacket[2] = (u8)((u32VehicleID & 0x000000FF)>>8);
                  u8TxPacket[3] = (u8)((u32VehicleID &
0x000000FF)>>16);
                  u8TxPacket[4] = (u8)(u32PreviousReaderID &
0x000000FF);
```

```
                  u8TxPacket[5] = (u8)((u32PreviousReaderID &
0x000000FF)>>8);
                  u8TxPacket[6] = u8VehcileData;
                  RadioStartTransmit(u8TxPacket, 14);
                  u32PreviousReaderID = u32CurrentReaderID;
               }
            break;
            default:
            break;
            }
         }
      }
   }
}
```