AN INTELLIGENT ARCHITECTURE FOR METROPOLITAN PARKING CONTROL AND TOLL COLLECTION

“IMPACT”

By

SHOBHIT SHANKER

DISSERTATION

Submitted to the Graduate School

of Wayne State University,

Detroit, Michigan

in partial fulfillment of the requirements

for the degree of

MASTER OF SCIENCE

2005

MAJOR: COMPUTER ENGINEERING

Approved by:

Syed Masud Mahmud March 21, 2005

Advisor Date
ACKNOWLEDGEMENTS

I would like to express my deep felt appreciation to my advisor Dr. Syed Masud Mahmud, who has always invested his confidence in my ideas and abilities. It has been an honor to work with such an elite person who possesses such exceptional insight into various research fields and has throughout my thesis work helped me out in terms of valuable guidance. This research work could not have been accomplished without his constant guidance. I also thank my thesis committee member Dr Pepe Siy and Dr Feng Lin for their time and support. Finally, I want to thank all my friends at Wayne State University who have made my study and work a great pleasure.
## TABLE OF CONTENTS

ACKNOWLEDGEMENTS...........................................................................................................2

LIST OF TABLES.....................................................................................................................6

LIST OF FIGURES ...................................................................................................................6

1. INTRODUCTION ..................................................................................................................9

   1.1 BROAD ISSUES AND CONCERNS ...............................................................................10

2. LITERATURE REVIEW ......................................................................................................12

   2.1 MAIN OBJECTIVES ....................................................................................................12

   2.2 PROPOSED SYSTEM ..................................................................................................14

   2.3. BACKGROUND MATERIAL .....................................................................................16

      2.3.1 SOME APPLICATIONS OF MOBILE PHONES TO TRAFFIC MANAGEMENT AND CONTROL ...........................................................................16

      2.3.2 NEXT-PARK ........................................................................................................17

      2.3.3 SMART-PARK ....................................................................................................18

      2.3.4 Park and Display & Pay by Space .......................................................................18

      2.3.5 The MPAY project .............................................................................................19

      2.3.6 DSRC (Dedicated Short Range Communication) ..................................................20

3. PROPOSED ARCHITECTURE ...........................................................................................21
3.1 FIRST LAYER (CONNECTION ESTABLISHMENT PROTOCOL)........22

3.2 SECOND LAYER (SECURITY PROTOCOL)...........................................22

3.3 THIRD LAYER (IMPACT PROTOCOL).................................................22

3.3.1 AD-HOC SUBSYSTEM.................................................................24

3.3.2 PARKING GATEWAY SUBSYSTEM.................................................25

3.3.3 VEHICLE DETECTION SUBSYSTEM...............................................27

3.3.4 VIDEO IMAGE PROCESSOR SUBSYSTEM.......................................29

3.3.5 CONNECTION ESTABLISHMENT PROTOCOL...............................30

4. IMPACT PROTOCOL........................................................................31

4.1 FALSE ALARM DETECTION.............................................................33

4.2 IMPACT AS DRIVER ASSISTANCE SYSTEM....................................35

4.3 SECURITY PROTOCOL....................................................................36

4.3.1 PKI (PUBLIC KEY INFRASTRUCTURE).......................................37

4.3.2 KEY AND CERTIFICATE MANAGEMENT..................................38

4.3.3 TWO CHAIN OF CERTIFICATES................................................39

4.4 AUTOMATIC CHARGING TECHNIQUE FOR THE VEHICLE.........40

4.4.1 AUTHENTICATION MECHANISM.................................................43

4.4.2 AUTHENTICATION FOR THE USER AND PARKING GATEWAY......43
LIST OF TABLES

TABLE I: Revenue generation from street parking in 4 major U.S metros

TABLE II: Bandwidth requirement with increase in the % of warning message

TABLE III: Bandwidth requirement for parking gateway with the increase in parking meters under its range

TABLE IV: Bandwidth $B_p$ required by the parking gateway to accept messages

TABLE V: Time required by the vehicle during PG authentication

TABLE VI: Memory requirement for Parking Gateway

TABLE VII: List of parameters used in performance analysis

LIST OF FIGURES

Figure 1: Layered architecture of IMPACT

Figure 2: IMPACT with its components

Figure 3: State diagram of the parking meter
Figure 4: The architecture of the IMPACT system.................................26
Figure 5: The sensors of the IMPACT system........................................33
Figure 6: Flow chart for IMPACT protocol..........................................35
Figure 7: Version 3 public key certificate..............................................38
Figure 8: Certificate Chain...............................................................39
Figure 9: Flow Chart for debiting the toll amount for the account..........42
Figure 10: Format of digital certificate................................................43
Figure 11: Flow Chart for the authentication of Parking Gateway by the vehicle's
          to start accepting messages.....................................................45
Figure 12: Data packet for information on parking meter......................46
Figure 13: Data packet for information on status of parking meters........47
Figure 14: Inquiry packet sent by parking meter..................................48
Figure 15: Response packet sent by vehicle.........................................48
Figure 16: Data packets for information exchange between vehicles and
          meters..................................................................................49
Figure 17: Flow chart for e-ticket mechanism......................................51
Figure 18: Data transmission from parking gateway to parking server.....52
Figure 19: Layout of parking meters and gateway's in a typical metro
downtown.......................................................................................54
Figure 20: Radar based sensing mechanism for the vehicle
detection.........................................................................................56
Figure 21a: Format for information on parking space availability.........58
Figure 21b: Format for warning message for Class I vehicles..............59
Figure 21c: Format for warning message for Class II vehicles..........................59
Figure 22: Graph Indicating the increase in required Bandwidth with % of violation messages.................................................................62
Figure 23: Data packet format for information on number of available parking spaces.................................................................63
Figure 23a: Bandwidth $B_{b}$ required by the gateway.................................................65
Figure 24: Time required for authenticating a Parking Gateway by all the vehicles within its range.................................................................69
Figure 25: Distance a vehicle can travel during authentication process for different PG ranges..................................................................70
Figure 26: Distance a vehicle can travel during authentication process for different PG ranges..................................................................71
INTRODUCTION

Parking is a critical component of transportation policy and management for any locale, but especially for the large central cities. The infrastructure associated with parking calls for major planning and policy decisions. The policies and management practices affecting parking lead to outcomes that, in turn, can affect land use, air quality, traffic congestion, travel behavior, safety, and economic development, not to mention revenue lines. Due to ever-increasing pressure on the major cities for parking spaces, effectively managing parking is an ongoing battle as they face competing, and sometimes contradictory, objectives.

Table I illustrates the amount of revenue generated from street parking in 4 major U.S metros.

<table>
<thead>
<tr>
<th>Sr.No</th>
<th>City name</th>
<th>Revenue (In million dollars)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Dallas</td>
<td>2.9</td>
</tr>
<tr>
<td>2</td>
<td>Portland</td>
<td>2.5-3.0</td>
</tr>
<tr>
<td>3</td>
<td>Los Angeles</td>
<td>92.7</td>
</tr>
<tr>
<td>4</td>
<td>Chicago</td>
<td>112</td>
</tr>
</tbody>
</table>

Table I: Revenue generation from street parking in 4 major U.S metros.
1.1 BROAD ISSUES AND CONCERNS

Street parking has many interrelated, though not always integrated, elements, both in the policy and operations areas. It is not sure how the interrelation of street parking is to broader issues of land use, economic development, and travel behavior. Also not much of research has been done as to how the enforcement tasks are carried out with how much revenue. Much of the research dealing with parking operations uses a case study approach, often detailing just one case. Thus, while cities can often point to areas of difficulty, finding solutions is not simple. Some of the most critical street parking problems are:

• Lack of availability of parking spaces: While the most common statement was something like that of New York City – “too many vehicles, not enough spaces,” – others, like Dallas, noted problems with downtown spaces, and some, like Los Angeles, pointed to a lack of residential spaces, in particular.
• **Juggling multiple interests**: Residents, visitors, businesses, and other groups all have different needs and desires when it comes to street parking. Determining the best mix for serving these interests is critical, but not easily accomplished.

• **Abuse of permits for disabled persons (ADA parking permits)**: There are many instances of persons without disabilities making use of reserved spaces as well as misusing ADA permits. For several cities there are state mandated requirements that also lead to difficulties with legitimate ADA permits being used for long-term metered street parking, thus limiting turn-over. For example, Oregon state law mandates all-day free street parking for persons with disabilities.

• **High levels of idling with resulting emissions**: With street parking in high demand and insufficient spaces, many drivers wait for spaces to become available.

• **Replacing obsolete technologies**: There are many new technologies available for street parking, but there are also financial and political hurdles that must be overcome.

Street parking generates significant revenues for cities, both through regular fare collection and fines. The annual revenues from street parking for 4 major U.S metros were anywhere from $2.9M (Dallas) to $112M (Chicago) each year. The research on revenue from street parking was done in 7 cities. The annual revenues from street parking for Portland and Dallas were on the lower end of
the scale at $2.5-$3M and $5.4M, respectively, while for Los-Angeles and Chicago were at the higher end of the spectrum, reporting $92.7M and $112M [1]

2. LITERATURE REVIEW

U.S Federal and State governments invest millions of dollars for enforcing parking control in metro city areas. Tasks like parking enforcement, towing of illegally parked vehicles and maintenance require many man-hours and resources. The parking control and revenue system in the metro are essentially dependant on devices like coin or token based parking meters that require the use of exact change and is cumbersome. Also patrol officers are required to monitor these spaces constantly. This entails the need for a more efficient and redundant system. In this thesis, an architecture for automated parking meter and driver assistance system is proposed that shall be connected to a centralized traffic control authority responsible for parking enforcement and toll collection. This system would provide a more efficient and redundant way of enforcing parking control and toll collection and also assist drivers in metro areas for searching an available parking space. The above-mentioned architecture enables automated parking toll collection.
2.1 MAIN OBJECTIVES

The main objectives of parking control and enforcement systems include efficient and effective monitoring of meter and lot violations. The aim is to provide adequate space for parking in downtown/metro city areas and optimize the use of all city parking spaces to maximize revenue. To achieve these objectives, further development and upgradation of the present parking system is required. The parking authority has to employ personnel for enforcing the regulations; some of these include police officers, parking control technicians and maintenance personnel. The above-mentioned services add up to make significant cost.

The parking meter services include meter and zone enforcement, meter maintenance, meter collections and debt services. The revenues from these go into the overall improvement of the parking enforcement infrastructure. According to the estimates done by the parking enforcement office of the city of Lawrence, Kansas [2] it would take $700,000 - $800,000/year to enforce the parking control in its metro area. These costs include, employing the manpower apart from the resources like patrol vehicles, gasoline, towing trucks, etc. Lot of man-hours is spent in enforcing parking control and related activities such as towing of illegally parked vehicles.

The parking toll collection in metro areas is mainly based on the coin or token-based parking meter systems [3]. The coin-based meter requires the use of exact change and is a quite cumbersome process, because the user has to tender
exact change in order to park. During odd times like night or wee hours or some
events when there is scarcity of parking, it is quite troublesome to look for
parking space elsewhere, due to lack of change. In such an event, the driver
would not be fully aware of existing parking spaces nearby and it would be very
time-consuming and frustrating for the driver to look for one. This requires the
need for developing a parking toll system, which shall be free from all the above-
mentioned issues and would be user friendly, efficient and redundant. Also it is
important that such a system should exist on top of or be an up gradation of the
existing architecture, because it is not feasible to implement a totally new system.

2.2 THE PROPOSED SYSTEM

The proposed system is called Intelligent architecture for Metropolitan PArking
Control and Toll collection (IMPACT). In this system, the use of a wireless device
with a software function that shall be embedded in the parking meter and would
be having wireless ad-hoc networking capabilities is proposed. It is also proposed
that the parking meter be embedded with two frequency modulated continuous
wave (FM-CW) radar sensors and a low cost video camera. These two sensors
ensure vehicle detection and that the driver has parked his/her vehicle in the
correct place. The small video camera is placed to eliminate the possibility of
false alarms. A tower, known as the Parking Gateway (PG), shall be wirelessly
linked to all the parking meters and would act as a gateway between the parking
meters and the centralized parking authority.
The architecture enables more effective monitoring of parking lot violations through the use of radar sensors and wireless ad-hoc networking. It shall notify the central parking authority about a meter violation automatically without the interface of a patrol officer. This shall be explained in the latter sections. Since our system is fully automated, it eliminates human error and is therefore more redundant and efficient. The proposed system also provides a better revenue model for the parking authority. Ad-hoc wireless networks are used for communications between vehicles and parking meters. In future, it is assumed that all the cars shall be enabled with a wireless networking capability and would be able to wirelessly exchange data with other devices in its vicinity. The architecture can be easily implemented by upgrading the present infrastructure. This means that it will exist as another layer on top of the present parking meter system architecture. This makes it scalable for future system up-gradation.

In the recent years, numerous mobile parking solutions [4, 5, 6] have been introduced all over the world. Wireless parking control combined with mobile payment is regarded as a promising concept for gaining added value to parking services. Since a majority of people or drivers have an interaction with a parking meter at least once in a day, it pays to search for wireless parking solutions, in which personal mobile phones or in-vehicle embedded devices could be used to interact with wireless ad-hoc networking devices embedded inside the parking meter. The common factor for all network-based wireless parking control and payment systems is, unfortunately, that the utilization of network services, like phone calls or messaging, are a cause of excess costs. These costs finally fall on
the parkers themselves. In addition to connection fees, many wireless parking solutions have also additional fees like use charges, registration fees and separate bill fees. It is essential to the wireless parking system to be user-friendly in order to become adopted by parkers. Some previous architectures have suggested the use of cell phones for the parking solutions. The use of cellular network based parking solutions require memorizing at least the service phone numbers, which may also vary by parking area, and possibly the correct message formats in SMS, based services [5, 6]. Since the recognition of vehicles in many wireless parking control and payment systems is based on plate numbers, pre-registered drivers using several different cars face problems in using these systems.

Due to drawbacks in existing wireless parking services, it is worthwhile to search for an easy-to-use concept the use of which would also be free of charge. In this thesis one potential solution is presented based on utilizing services of intelligent transportation systems infrastructure.

The next section describes some background material about current architectures for parking control. After that a description of the proposed architecture is presented. System requirements, bandwidth analysis, conclusions and future work are presented at the end of the thesis.
2.3 BACKGROUND MATERIAL

2.3.1 SOME APPLICATIONS OF MOBILE PHONES TO TRAFFIC MANAGEMENT AND CONTROL

Many new features will open to network traffic control and management when traveler information systems and navigation will be integrated into a single phone terminal. Phones will be connected to a car navigation terminal and a multimedia interface via IR data transmission (or the new Bluetooth short distance radio standard), or the phone in itself will have this capacities. Parking operations could be completely automated. Payments will be effectuated by phone using encrypted short text messages, and parking spot availability will be known in advance allowing drivers to avoid searching full parking lots. Using automated systems, cities and road management authorities will be able to adjust toll for congested roads so as to avoid environmental emergencies. One of the big potential benefits of mobile data phones in traffic management is the possibility of collecting toll from car drivers avoiding queues. All those applications will be applied only when standardization will emerge and will be reached with the convergence of internet into digital mobile phones [7].

Some of the current parking and toll architectures that are in use are NextPark [8], SmartPark [9] Park-and-Display [10] and Pay-by-Space [10], MYPAY [11, 12]. These are described here:
2.3.2 NextPark

This is a new architecture for parking control that is implemented in Finland by the Oulu Telephone Company. It makes use of the GSM mobile phone network to monitor the whole metro area for parking enforcement. In this system, the user registers on the Telephone Company's website and gets a unique ID or PIN. When the motorists want to park they dial NextPark number. Once they are identified they are asked for details like the parking zone and the amount of time they need to park. This information is then forwarded to the NextPark server that confirms all the details and chooses to accept or modify them. When the patrol officer enters the zone he/she dials the NextPark number, the server responds giving the details about the vehicles allowed parking time, license plate number. It warns the owner 15 minutes before the parking time expiration and is asked if he wishes to extend the time.

2.3.3 SmartPark

This technology requires the use of In-Vehicle Car Parking Meters or ICPM [13]. The ICPM is a small pocket calculator-size electronic device. This SmartPark device uses a smartcard that's loaded with a prepaid amount of parking hours. The smartcard is inserted into the SmartPark, which is then placed inside the vehicle and displays the parking time purchased. An initial one-time refundable deposit for the SmartPark unit is $55 and customers must purchase the smartcard for $10. Customers can preload the Smartcard in increments of $25,
$50, $75 and $100. The SmartPark is then placed inside the vehicle and displays the parking time purchased.

### 2.3.4 Park-and-Display and Pay-by-Space

The park-and-display [14] version is used in France. In this system, the driver deposits the money and the machine prints a receipt with the expiration time. The receipt is pasted on the Dashboard for the meter reader to see. The second is a pay-by-space method in which drivers deposit money for their numbered space. A red light by a number on the monitor indicates that the corresponding parking space has expired.

### 2.3.5 The MPAY project

The MPAY project was a jointly funded project targeted to implement and pilot a parking control system based on utilizing local wireless services. The leader of the project was Tampere Parking Houses Ltd [11], a significant Finnish parking operator and parking equipment distributor in Scandinavia and Baltic Countries. The other co-operative partners were Nokia Mobile Phones Ltd [12], the leading mobile phone manufacturer in the world, and VTT Information Technology [15], a governmental research organization doing research in the field of microelectronics, information technology and media technology. In addition, the project was co-financed by Finnish Technology agency [16] that finances R&D projects of companies and universities in Finland.
The name of the project, MPAY, is short form for the term "mobile payment" meaning wireless transactions for paying goods or services on the move. Despite of its name, the research subject of the project was predefined to comprise service concepts enabling wireless parking control, payments and guidance. At the time of project launch, no solutions utilizing mobile phones in car parking had been introduced [17]. The basic idea of the project was to apply local wireless services in car-park solution to pilot a network operator independent of means of wireless communication between parkers and parking control system. The objective was to define, design and implement a hardware and software configuration enabling both access control of short-term and season parkers, and simulation of wireless cash payments by mobile phones. The basic idea of the new concept was not to bring another billing variant for car park users but to introduce new diversified services for them and to make car park access more comfortable and fluent.

2.3.6 Dedicated Short Range Communications (DSRC)

5.9 GHz DSRC (Dedicated Short Range Communications) is a short to medium range communications service that supports both public safety and private operations in roadside-to-vehicle and vehicle-to-vehicle communication environments. Dedicated Short Range Communications (DSRC) [18] allows high-speed communications between vehicles and the roadside, or between vehicles, for ITS; it has a range of up to 1,000 meters [19]. Potential DSRC applications for public safety and traffic management include:
• Intersection collision avoidance
• Approaching emergency vehicle warning
• Vehicle safety inspection
• Transit or emergency vehicle signal priority
• Electronic parking payments
• Commercial vehicle clearance and safety inspections
• In-vehicle signing
• Rollover warning
• Probe data collection

3. THE PROPOSED ARCHITECTURE

The following diagram shows the layered architecture of the IMPACT protocol:
The protocol has a layered architecture and consists of three layers that are described as follows:

### 3.1 First Layer (Connection Establishment Protocol)

It consists of a connection establishment protocol, this layer deals with the ad-hoc networking between the in-vehicle wireless unit and the parking meter.
through ad-hoc wireless links (in this case we assume that these are Bluetooth links). The connection establishment protocol also has in-built security procedures [20] but, in the protocol we have not taken them into consideration. The security of the transactions over the wireless links is taken care of by the implementation of certificate technology and public key infrastructure (PKI) [21] that utilizes the pair of public and private key pair. This implementation is based in the second layer and this layer stays on top of the connection establishment layer.

3.2 SECOND LAYER (SECURITY PROTOCOL)

The second layer consists of the security protocol implementations. As mentioned earlier this layer utilizes security techniques using digital certificate technology and public and private key pair technology. This layer stays on top of the connection establishment layer.

3.3 THIRD LAYER (IMPACT PROTOCOL)

The third layer consists of the protocol implementation in which the actual implementation of the hardware and software functions takes place. This layer defines the actual bit rates that are required for the transactions, the bandwidth requirements, and physical layer implementations.
Figure 2 shows the proposed architecture with its components. Here we present and discuss the Intelligent architecture for Metropolitan Parking Control and Toll collection or IMPACT. We have assumed that, within a metropolitan area, there will be a well-defined network infrastructure for Intelligent Transportation Systems (ITS) [22]. The ITS devices will be ubiquitous and would be performing multiple functions. We also assume that ITS infrastructure would be on top of existing infrastructure like the internet or the mobile network. Our architecture has the following sub-system entities:
3.3.1 AD-HOC SUBSYSTEM

This would consist of a device with wireless ad-hoc networking capabilities [23] and would be embedded in each of the parking meter. This device would be connected wirelessly to all the neighboring parking meters through its ad-hoc networking capability.

The ad-hoc subsystem would consist of low cost low power ad-hoc devices e.g. Bluetooth that shall be constantly on the lookout for a certain class of devices that is represented by the vehicles’ on board unit (OBU). The OBU is also equipped with the capability of ad-hoc networking. The ad-hoc device shall constantly be going on through the process of Inquiry through which it constantly looks out for the vehicles’ OBU class of device; this process is called as an Inquiry sequence. Through the Paging sequence the device actually gets connected to the vehicle. Figure 3 [20, 23] is the state diagram of the parking meter, which is an ad-hoc device. The Figure 3 describes the various states in which the ad-hoc device i.e. the parking meter would be.
3.3.2 PARKING GATEWAY SUBSYSTEM

This would be a tower located at various locations of the metro area and would be linked to all the parking meters in its vicinity. Each parking meter would be having a unique ID or a number associated with it. The gateway would link all the parking meters to the centralized server of the parking authority. The parking gateway shall be directly linked to server or if its out of range of the server than it could use an ITS entity like an Intelligent Transportation Tower, which would be responsible for many other functions apart from routing information, such as parking meter ID, to the centralized server. The purpose of routing the parking meter ID or PID to central server is to keep track of the information related to that
particular parking space such as illegally parked vehicles, available parking space at that location etc. The parking gateway could be Wi-Fi [24] router linked with all parking meters and further connected through a Wi-Max connection to the central parking server.

![Diagram of the IMPACT system]

**Figure 4: The architecture of the IMPACT system**

The parking gateway also performs the function of beaming the available parking space information on air. This is done using broadcast transmission at the frequency of 5.9 GHz, DSRC communication range which is the industry standard for roadside to vehicle communication and inter-vehicle communications. The parking gateway keeps on broadcasting the status of available parking spaces in its vicinity. The vehicle, as soon as it enters the metro area communicates with the gateway through its on-board wireless unit. Thus it gets real-time information about the available parking spaces. It is important that the wireless link between the gateway and the vehicle be secure. This can be
done by the certificate technology that shall be explained in later section of security.

### 3.3.3 VEHICLE DETECTION SUBSYSTEM

The vehicle detection subsystem uses the vehicle detection technology [25] to detect the vehicle when it is in the parking space. This subsystem is embedded on the parking meter itself and consists of two sensor one a microwave radar and other a laser sensor assembly which sense the presence in the manner described below.

The frequency modulated continuous wave (FM-CW) microwave radar sensor transmits a frequency that is constantly changing with respect to time. The FM-CW radar operates as a presence detector. The FM-CW radar sensor and laser sensor, Sensor-1 and Sensor-2, are used for each parking meter. The beam of Sensor-1 is pointed towards the center of the parking space and is required to check the presence of a vehicle. The output of Sensor-2 is monitored to check whether the vehicle has crossed its parking space and moved to the adjacent parking space.

The term microwave refers to the wavelength of the transmitted energy, which is usually between 1 and 30 cm. This corresponds to a frequency range of 1 GHz to 30 GHz. Microwave sensors designed for roadside traffic data collection and monitoring in the U.S. are limited by FCC regulations to operating frequency bands near 10.5, 24.0, and 34.0 GHz. The sensor manufacturers satisfy these
requirements, as well as others that restrict the transmitted power. Radars at frequencies above 30 GHz operate in the millimeter-wave spectrum since the wavelength of the transmitted energy is expressed in terms of millimeters. Commercially available microwave radar sensors used in traffic management applications transmit electromagnetic energy at the X-band frequency of 10.525 GHz. Higher frequencies illuminate smaller ground areas with a given size antenna and thus gather higher resolution data.

3.3.4 VIDEO IMAGE PROCESSOR (VIP) SENSOR SUBSYSTEM

This subsystem is also located on the parking meter and consists of very low cost camera that has the capability of taking the picture of the parking space. There are many low cost and compact cameras that are available under the price of $15 [26]. If these cameras were bought in wholesale then their price would be lower at about $8-10. The resolution for these cameras is 100,000 pixels. Some of these cameras also have a built-in memory to store images of size 2 MB. Thus, we might not be required to install memory for storing images on the parking meter. This system also roots out the possibility of false alarm due to the presence of stray object or malicious intent of someone. The camera can notify the central server about the presence of an actual car or other stray objects.

It is proposed that the video image processor have an algorithm embedded in it that would be detecting whether the image is that of a person or a vehicle.
3.3.5 CONNECTION ESTABLISHMENT PROTOCOL

The parking meter is an ad-hoc wireless device (in current architecture a Bluetooth device) that has to go through the steps of inquiry and paging, to get connected to the in-vehicle wireless devices. These are connection establishment procedures that are a part of the Bluetooth protocol. It is proposed that the connection establishment protocol can take place either way i.e. from the parking meter to the vehicles OBU or vice versa. In the architecture discussed it is assumed that the inquiry and paging procedures are initiated by the parking meter. Therefore in the connection establishment protocol the parking meter is always the master. It can be other way also for consideration. The Inquiry sequence is the procedure through which an ad-hoc device looks for a particular class of devices in its vicinity. In this state, the device sends an Inquiry packet addressed to either the General Inquiry Access Code (GIAC) or Dedicated Inquiry Access code (DIAC) which refers to a particular class of devices, in our case the in-vehicle embedded wireless device.

IMPORTANT NOTE: Please make an important note here, that the connection establishment protocol takes place through ad-hoc wireless networking (e.g. Bluetooth) that operates in the 2.4 GHz RF frequency range. Whereas the actual data communication for the Security and the IMPACT protocol takes place in the DSRC 5.9 GHz frequency range which is the industry standard for these applications. Here it’s assumed that the parking meter embedded device already knows the DIAC (Dedicated Inquiry Access Code) for the vehicles in-vehicular
embedded device. In ad-hoc wireless devices there are two states for each device:

MASTER: An ad-hoc device is called the master if it initiates a connection

SLAVE: An ad-hoc device is called a slave if it gets connected to another device that initiates the connection.
4. THE IMPACT PROTOCOL

Our architecture takes care of two classes of vehicles, Class-I and Class-II vehicles. The Class-I deals with current vehicles with no wireless devices embedded in them and that do not have the wireless ad-hoc networking capability. The Class-II vehicles will have an in-vehicle wireless device as an on-board unit (OBU) with ad-hoc networking capability embedded in them. Each of these vehicles would have a unique Vehicle Identification number (VID) assigned to them. A parking meter consists of two sensors that are embedded in it and are positioned at different angles, as shown in Figure 5. Sensor-1 consists of a laser beam or an infrared beam that is pointing to the direction pointing towards the pavement. Sensor-2 is a FM-CW radar sensor that is pointing towards the center of the parking space. The ad-hoc subsystem goes through the connection establishment protocol explained in the previous sections. If the parking meter detects a device with the DIAC it knows that a Class-II vehicle is nearby. After the connection has been made, it checks whether there has been an output detected from the sensor assembly. If the output is from laser Sensor 1 it knows that the vehicle is not parked properly because it has crossed the parking space boundary and reached into an adjacent space. It issues a warning to the vehicle’s driver through an audio message or a flash signal. This tells the driver that he/she should prepare to back up into the proper parking space. It time stamps this event by a parameter $T_v$ (vehicle entry time) and waits for a specific time interval known as wait period, $T_w$. We propose that the wait period $T_w$ would be longer than the average time needed to park a vehicle in a parking space.
When the vehicle owner (in our case the vehicle owner is the person driving the vehicle) returns and turns on the engine and leaves the parking space the meter comes to know about this through the radar sensor and calculates the toll. It then debits the amount for the toll from the vehicle owner’s account. The amount is deducted from the type of account the vehicle owner has. We propose the use of two types of accounts. One would be pre-paid account known as e-park and other would be through credit card transactions. The information about the type of account is communicated to the meter as soon as the vehicle comes in the vicinity. These payment type and the methods for deducting the toll and generating ticket information are further discussed in Section 4.4.

For Class-I vehicles, the parking meter ad-hoc subsystem goes through the regular process of inquiry. It looks for Vehicle Identification Number (VID). If it does not detect a VID but gets a response from the radar assembly it knows that the vehicle is Class-I vehicle. The meter checks this with the camera output to see that the output is actually generated by the vehicle and not due to the presence of some stray object or malicious intent of someone. This is done to eliminate the possibility of a false alarm. It time stamps this event and stores the vehicle entry time $T_v$ in its on-board memory. After that, the meter waits for the waiting period $T_w$. Then the meter checks whether any toll has been deposited and starts counting time for which the vehicle has been parked. If it does not receive the toll after $T_w$, then it sends the warning message to the PG and through that to central parking server about the parking violation at that spot. The warning message also consists of an image file of the license plate number of the
vehicle which is basically the snapshot taken by the camera installed at the adjacent parking meter facing in the direction of the back of a vehicle. If the vehicle is legally parked, the parking meter calculates the parking time according to the change put in the meter. If the vehicle overshoots the meter time, the meter notifies the main server using the same procedure mentioned in section 4.4. Figure 6 shows the flow chart of the IMPACT protocol.

Figure 5: The sensors of the IMPACT system

4.1 FALSE ALARM DETECTION

This section discusses the technique of false alarm detection by the parking meter. Figure 5 shows the top view of a parking lot. False alarms can be generated by the malicious intent of a person or accidentally by a pedestrian who might be standing at the parking spot. The system protocol eliminates such an alarm in the following manner. When the system detects the output from Sensor-2, i.e. the FM-CW radar sensor that is pointed to the center of the parking space,
it checks the output from the video image processor. If the camera does not detect a vehicle, it knows that it’s a false alarm and informs the system about it.

For a Class-I vehicle, send a warning signal to the central server with a picture of the license plate of the vehicle. For a Class-II vehicle, send a warning signal with the VID of the vehicle.
4.2 IMPACT AS A DRIVER ASSISTANCE SYSTEM

The IMPACT architecture can be used as a driver assistance system for parking in a metro area where it is difficult to find a spot. In this architecture each parking meter would be periodically sending its parking status, i.e. whether it is vacant or occupied, to the nearest parking gateway. The parking gateway then sends that information to the centralized server. Thus, the centralized server and all parking gateways are aware of the availability of the parking spaces within a particular area, such as near a stadium, shopping center, bus station, airport, etc. This information is beamed by the parking gateway using broadcast transmission in the DSRC frequency range of 5.9 GHz or any other frequency range that a vehicle can tune in too when entering a metro area and can know about the parking spaces. This way, as soon as a vehicle enters a particular area, it will get information in real-time about the availability of nearby parking spaces. This infrastructure can be further improvised in the way that a user can input its location and send a query message to the server. The server in turn, responds with parking space available within the vicinity of the vehicle.
4.3 SECURITY

In the architecture proposed all the data links are using wireless communications. For this purpose the DSRC 5.9 GHz roadside to vehicle communication channel has to be used. These links are present all over the air that they use as physical media of transmission. These links are vulnerable to attacks of security such as the man-in-the-middle attack [27]. Such attacks can render the system susceptible to failure and can wreck havoc to the parking control infrastructure. Also it can lead to privacy attacks on the vehicle owner e.g. knowing the vehicles location and transmitting this information over the air. Otherwise, the parking areas would be the playgrounds of various types of hackers. The sensor based wireless ad-hoc links among the parking meter, vehicle, and the parking gateway must be secured. Otherwise, hackers may inject wrong information into the system; read the VID number of a vehicle by eavesdropping on the link between the vehicle and the corresponding parking meter. Later on, the hackers may use this VID number to park his/her vehicle without paying any toll.

To make this system secure we need to incorporate some security techniques in our protocol. Some of the current security architectures have already been discussed in the literature review section. They are discussed in the following sections:

4.3.1 PUBLIC KEY INFRASTRUCTURE (PKI)

In this architecture we would require the use of two sets of keys: one is the public key and the other is the private key. Public-key cryptography is a key-factor for
the solution of the transaction security problems arising with the commercial use of the Internet: authenticity, integrity, confidentiality and non-repudiation [28, 29]. Public key cryptography is based on the use of key pairs. When using a key pair, one of the keys, referred to as the private key is kept secret and under the control of owner. The other key, referred to as the public key, can be disseminated freely for use by any person who wishes to participate in security services with the person holding the private key. The private key and the public key are mathematically related but it remains computationally infeasible to derive the private key from the knowledge of public key. In theory, any individual can send the holder of a private key a message encrypted using the corresponding public key and only the holder of the private key can decrypt the secure message. Similarly, the holder of the private key can establish the integrity and origin of the data he sends to another party by digitally signing the data using his private key. Any one who receives the data can use the associated public key to validate that it came from the holder of the private key and verify the integrity of the data has been maintained.

4.3.2 KEY AND CERTIFICATE MANAGEMENT

The distribution and management of the public key is the crucial point in the procedures described above. It must be guaranteed that the key really belongs to the respective person (or e-mail address or authorization role). A means to guarantee this is the use of digital certificates. They are digital documents
containing the public key, the name of the possessor, the digital signature of the certification authority (CA) [29] that issued the certificate and the certificate validity period. Figure 7 illustrates the Version 3 public key certificate as defined in X.509. In this way the problem of key management is reduced to the public key of the CA. Once in possession of the trustworthy public key, the end user is able to verify all certificates issued by the certification authority. The function of a CA is therefore the verification of the identity of the certificate holder.

<table>
<thead>
<tr>
<th>Version</th>
<th>Serial Number</th>
<th>Signature (Info)</th>
<th>Issuer</th>
<th>Validity</th>
<th>Subject</th>
<th>Subject Public Key Info</th>
</tr>
</thead>
</table>

- Issuer Unique ID
- Subject Unique ID
- Optional Extensions
- Digital Signature

Figure 7: Version 3 public key certificate

4.3.3 TWO CHAINS OF CERTIFICATES

Two chains of certificates shall be required to authenticate the vehicle and the parking meter. In the architecture, unidirectional chain of certificates are used for validating the parking gateway and parking meter messages in which USDOT [30] acts as a certifying authority and is trusted by everyone. During the manufacturing of the vehicle, the USDOT’s public key is embedded in the vehicles OBU. USDOT issues and signs a certificate for each state parking
control authority. Each state acts as a certifying authority and signs a certificate for each county parking control. Each county acts as a certifying authority and signs a certificate for each city and each city acts as a certifying authority and signs a certificate for each metro or parking gateway and parking meter. A parking gateway and parking meter are issued a key pair (private, public) by its city. This key pair is embedded in their hardware. For a PG and parking meter the certificate chain looks like the one shown in Figure 8.

<table>
<thead>
<tr>
<th>..</th>
<th>..</th>
<th>..</th>
<th>US DOT</th>
<th>..</th>
<th>..</th>
<th>..</th>
<th>STATE PARKING ID</th>
<th>Digital Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>..</td>
<td>..</td>
<td>..</td>
<td>STATE PARKING ID</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>COUNTY PARKING ID</td>
<td>Digital Signature</td>
</tr>
<tr>
<td>Equal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>..</td>
<td>..</td>
<td>..</td>
<td>COUNTY PARKING ID</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>METRO PARKING ID</td>
<td>Digital Signature</td>
</tr>
</tbody>
</table>

**Figure 8: Certificate Chain**

### 4.4 Automatic Charging Technique for the Vehicle

When a vehicle is manufactured, at that time its OBU will be embedded with the necessary information needed for all the operations on a daily basis. There shall be two ways to automatically charge the vehicle for parking toll transactions:

1. Using the Credit card information of the user

2. E-Park Credits
CREDIT CARD BASED CHARGE

When the car owner enters a parking space he/she will be asked about their intention to park. If the user intends to park then he/she shall be asked to furnish the information about the credit/debit card. This information would be sent to the central parking server and stored in the memory associated with that particular vehicle’s VID. When the customer actually parks the vehicle in front of the parking meter, at that instant onwards the parking meter starts counting the time of the vehicles occupation of the space. When the customer returns the actual money is deducted for the credit/debit card information furnished by the user. If the credit card number is declined for any reason it shall ask the customer for another credit card. In case the transaction doesn’t go through an e-ticket can be generated.

E-PARK CREDITS

The second option that we have devised is using E-park. In this option, the customer can purchase some parking credits online by setting up an E-Park account online. When the parking credits are purchased the OBU stores the credit information. These credits can be used anywhere in the country and would be recognized as currency by the parking authorities or USDOT. So once the customer has bought the E-Park currency it can recharge its OBU with parking currency.
Scenario 1: The driver has parked his car and has gone to attend meeting:

Take the case of Scenario 1 in which the user who has bought the credits and his parking time exceed the limit of his existing credits. In such a case an e-ticket is generated in the vehicle owner's name and sent to state authority. The e-ticket is same as a normal parking ticket but generated and issued electronically. Therefore, for e-park the user has to ensure that the e-park account has sufficient credits, e.g. for using a credit card the user has to ensure that account has sufficient money.

In future this protocol might be changed and additional E-park credits could be automatically issued to the user and credited to his E-Park account. When the user returns, these credits are charged to his E-Park account number.

The following flow chart in the Figure 9 demonstrates the algorithm:
Figure 9: Flow chart for debiting the toll amount from the account.
4.4.1 AUTHENTICATION MECHANISM

4.4.2 Authentication for the user and the parking gateway

Since using these wireless connections and automatic charge mechanism we are
transferring sensitive information such as credit information and bank account
information of the driver, it is imperative that the whole transaction be secured
and authentication of PG by the vehicle be taken into consideration.

The authentication between the vehicle and the parking infrastructure can be
done by using the certificate technology. The parking infrastructure entities such
as parking meter and parking gateway will have certificates embedded inside
them that shall be signed using the private key of the metro county parking
control authority which in turn shall be signed by the state and USDOT. The
parking gateway and parking meter are on the same level of hierarchy and
therefore use the same certificate and secret key. This way the authentication
process goes through two chains of certificates and in this way the parking
infrastructure entities can be authenticated. The Figure 10 below shows the
format of a digital certificate:

<table>
<thead>
<tr>
<th>S</th>
<th>O</th>
<th>M</th>
<th>Hierarchy Level</th>
<th>Issuer ID</th>
<th>Validity</th>
<th>Subject ID</th>
<th>Public Key</th>
<th>Digital Signature</th>
<th>CRC</th>
<th>EOM</th>
</tr>
</thead>
</table>

**Figure 10: Format of a digital certificate**

The flow chart in the Figure 11 explains how the process takes place:
Start

Is the vehicle in range of parking gateway?

Yes
Request the Parking gateway for its State certificate & check the validity of the certificate

No

Is the certificate valid?

Yes
Extract the Public key of state

Request the Parking gateway for its County certificate & check the validity of the certificate

No

Is the certificate valid?

Yes
Extract the Public key of County
Figure 11: Flow chart for authentication of the Parking Gateway by vehicles to start accepting messages
4.5 DATA PACKET FORMAT
4.5.1 INFORMATION EXCHANGE BETWEEN THE PARKING GATEWAY, VEHICLES AND PARKING METERS

The parking gateway continuously beams information to the vehicles about the availability of the parking space. A vehicle receives this information after it has gone through the authentication mechanism with the PG. The authentication mechanism between the vehicle and the meter follows the same procedure as between the vehicle and the parking gateway. The data packet contains information about the street name of the parking meters. This information is represented by the 16-bit identifier or PID of the parking meter as shown in Figure 12.

Let's say each parking gateway has 1000 parking meters in its range. Each broadcast data packet will contain the following bits:

- P1, P2…..P_n = 1000*16 bits = 16000 bits = 2000 bytes
- CRC = 16 bit
- SOM and EOM = 16 bits each

Total length = 2006 bytes
Therefore 2006 bytes have to be sent over the air for the vehicles in the vicinity of the parking gateway to know about the status of parking spaces in that area. The parking gateway also gets real-time information about the status of the parking meters availability for space. The parking meters, as soon as they get occupied by the vehicles, send this information to the PG and when the vehicle leaves the parking space the parking meter updates this information to the PG. In Figure 13 is the format of the data packet that is sent by the meter to the gateway periodically for updating the information on its availability for parking:

<table>
<thead>
<tr>
<th>SOM</th>
<th>PARKING STATUS</th>
<th>PID</th>
<th>CRC</th>
<th>EOM</th>
</tr>
</thead>
</table>

**Figure 13: A Data packet for information on the status of a parking meter.**

The SOM and EOM fields are 16 bits long; the parking status field is 1-bit long that indicates the availability of that particular space; the PID is 16-bit long; the CRC field is 16-bit long. The total length is 65 bits.
4.5.2 DATA PACKET AND MESSAGE FORMAT FOR THE PARKING METER 
AND VEHICLE INTERACTION

The following are the formats of data packet message for the interaction between a vehicle and a parking meter. The following are the data packets that shall be exchanged between the vehicle and the parking meter when it comes in the range. When the vehicle comes in the vicinity of parking meter and the connection establishment protocol of the ad-hoc networking device has already been taken place, the parking meter first sends the vehicle a 16 bit PID identifier which is basically the information about the parking meter itself and an inquiry bit I which basically asks the vehicle about the intention to park. Figure 14 shows the data format.

<table>
<thead>
<tr>
<th>SOM</th>
<th>16 bit PID identifier</th>
<th>I (1 bit)</th>
<th>EOM</th>
</tr>
</thead>
</table>

**Figure 14: Inquiry packet sent by parking meter**

Data format for the response message packet sent by the vehicle in response to the packet sent by the parking meter is shown in Figure 15:

<table>
<thead>
<tr>
<th>SOM</th>
<th>VIN NUMBER (56 BIT)</th>
<th>Response bit for Park (1)</th>
<th>Payment type</th>
<th>CRC</th>
<th>EOM</th>
</tr>
</thead>
</table>

**Figure 15: Response packet sent by vehicle**

The parking meter after getting the response packet from the vehicle knows about the type of payment that shall be done by the user i.e. either an e-park account or credit card based transaction. If it’s an e-park account then the meter
asks the vehicle to send the information about the status of e-park credits in its account and starts debiting the credits as the time of parking increases. If the amount of toll goes above the number of e-park credits then an e-ticket is generated automatically for the vehicle.

When the vehicle leaves, the following information shown in Figure 16, is exchanged between the parking meter and the vehicle

| SOM | Toll amt (8 bits) | Time (8 bits) | Amt of E-park credits | Debit | EOM |

**Figure 16: Data format for information exchange between vehicles and meters**

The meaning of each field of the above-mentioned format is as follows:

Toll amt: The total amount of toll that the customer has to pay

Time: The amount of time the vehicle was parked

E-park: If the customer has an e-park account

Debit: The parking meter asks the owner about the consent to debit.

The vehicle responds with a similar packet informing the meter about its intention and also allowing it to debit the toll.
4.6 E-TICKETING MECHANISM-IDENTIFYING THE VEHICLE

One of the significant advantages of using IMPACT system is the increase of revenue for the parking control authorities and in turn for the USDOT. The architecture enables to generate the e-ticket for the violating vehicles. The following paragraph explains how the mechanism works.

As we have explained earlier in our protocol as soon as the driver of the vehicle comes near the parking meter he/she is asked by the meter about the intention to park. As soon as the driver parks, the parking time starts debiting the account depending upon the type of account they have. When the driver comes back he is asked about the money that he owes for the parking and whether it should be debited from the account. If the driver drives off without acknowledging, then his VID (vehicle identification number) will be tagged and an e-ticket is generated in his name. The information can then be transferred to the state department through which he can be notified. Simultaneously using the camera on top of the meter we can take a snap shot of the license plate number and send to the central server. This way the image file can be stored in memory of the server and reproduced for future reference. The flow chart in Figure 17 describes how the mechanism shall work:
Figure 17: Flow chart for e-ticket mechanism
4.7 DATA TRANSMISSION FROM PARKING GATEWAY TO CENTRAL PARKING SERVER

The parking gateway is similar in function to the mobile base stations in cellular communications and the central parking server is analogous to mobile telephone switching office (MTSO) [31] in cellular communications. If the parking gateway is in the range of the central server then the data can be sent directly to it. If the PG is out of the range then we can send the data packets through multiple hops using adjacent PG. The Figure 18 below describes how this communication shall take place.

Figure 18: Data packet transmission from parking gateway to server
As shown in Figure 18 above the two PG in green and brown color code are in the range of the server and hence can directly transfer the data packets to the server whereas the PG’s that are out of range from the server can send their data packets by routing them through the PG’s as shown in the Figure 18 with light blue dotted line. Each parking gateway shall maintain a routing table of the nearest available PG’s and thus shall know the routing information. This information can alternately be transferred through a Wi-Fi or Wi-Max router.
Figure 19: Layout of parking meters & parking gateway in a Metro
4.7.1 MODULE CHECKING

The ad-hoc networking device embedded inside the parking meter shall do a device check after every 10ms. The device checks to see whether its neighboring devices are present around it i.e. the device does a hardware check in its environment. If it fails to find the list of devices which should be present around it e.g. memory buffer or the interface module of the hardware for the web camera it automatically issues a warning to the central server that the meter has been tampered with or is faulty. This way the upkeep of the meters is done automatically on regular basis and also the meter becomes tamper resistant and can be prevented from giving faulty information.
4.7.2 SENSOR MECHANISM: Radar Based detection sensors

The radar based sensor sends the radar beam which is reflected off the ground surface.

In the presence of the vehicle the beam gets reflected and detected by the sensor.

Figure 20: Radar based sensing mechanism for vehicle detection

The following is a motion sensor is based on ultra-wideband (UWB) radar [32]. UWB radar range is determined by a pulse-echo interval. For motion detection, the sensors operate by staring at a fixed range and then sensing any change in
the averaged radar reflectivity at that range. A sampling gate is opened at a fixed delay after the emission of a transmit pulse. The resultant sampling gate output is averaged over repeated pulses. Changes in the averaged sampling gate output represent changes in the radar reflectivity at a particular range, and thus motion. Detection ranges from 1 to 10 feet are practical with omni directional antennas. The cost of the UWB module could be in the order of $10 [33].

5. PERFORMANCE ANALYSIS

The types of messages that are exchanged between the IMPACT entities in the protocol are as follows:

1) Parking Space availability: meter → parking gateway

2) Parking meter violation warning message: meter → parking gateway

3) Parking Gateway broadcast message to vehicles: parking gateway → vehicles

4) Parking Gateway authentication by the vehicles: vehicles ←→ parking gateway

The following parameters have been taken into consideration for the performance analysis:

a) Number of parking meter under one parking gateway (PG)

b) Number of violations or percentage of violations

c) Number of vehicles in the vicinity of the PG

ASSUMPTION: The parking meters and the parking gateway are on the same hierarchical level of certificate chain and therefore incoming vehicle can also
undergo authentication procedure with the parking meters. However, for the sake of analysis here we assume that all the incoming vehicles authenticate the PG first and therefore when they are near the parking meters they already have the meter’s public key for communications. Let’s consider the first message case:

1) Parking Space availability: meter → parking gateway

The Parking Gateway will have to broadcast (in real time) the information of the available parking spaces in its vicinity i.e. the available parking meters. The parking meters, as soon as the vehicles vacate them, send the information to the PG. The PG strips off the data packet and keeps just the PID of the parking space (vacant) in its memory. After sufficient numbers are stored in its memory it beams them over the air. The parking gateway keeps beaming the data packets over the air to the vehicles in its range. As explained in Section 4.5 the format of data packet sent by meters to PG is as shown in Figure 21a.

| SOM | PARKING STATUS | PID | CRC | EOM |

**Figure 21a: Format for information on parking space availability**

So if there are 1000 meters in a PG’s range and if 10% gateways are assumed to send the availability updates every second then 100 meters shall be sending 6500 bits. The parking gateway stores in its memory the PID information about all the available parking spaces in its vicinity.

2) Parking meter violation warning message: meter → parking gateway
5.1 BANDWIDTH CALCULATION

Consider again for example one parking gateway keeps a track of 1000 parking meters. Let’s say for a worst-case scenario 20% of the parking meters are giving out warning signals. Then the number of parking meters generating warning signals is 200. For Class I vehicles the format for warning message to the server is shown in Figure 21b.

<table>
<thead>
<tr>
<th>SOM</th>
<th>VID</th>
<th>PID</th>
<th>SECRET KEY</th>
<th>EOM</th>
</tr>
</thead>
</table>

Figure 21b: Data format for warning message for Class I vehicles

VID = 56 bit number,

PID = 16 bit number

SOM = EOM = 16 bit

SECRET KEY = 128 bit

For Class II vehicles the format of warning message is shown in Figure 21c.

<table>
<thead>
<tr>
<th>SOM</th>
<th>IMAGE FILE</th>
<th>PID</th>
<th>SECRET KEY</th>
<th>EOM</th>
</tr>
</thead>
</table>

Figure 21c: Data format for warning message for Class II vehicles
PID= 16 bit number,

IMAGE FILE = 250,000 bytes

SOM=EOM =16 bit

SECRET KEY = 128 bit

CRC= 16 bit

The bandwidth and memory requirements mainly depend on the type of video camera and the image size that we use for the IMPACT system. The use of a very low-cost camera with a resolution of 500 X 500 pixels should be good enough for taking a picture of the license plate of a vehicle. If chosen to use black and white pictures with 256 gray levels, then a memory of size 250,000 bytes is needed for the picture. Apart from this, 10-20 bytes of extra information would be sent along with the vehicle’s picture. These extra bytes would include information like parking meter number, VID of vehicle, etc. Since this information is not processed in real time, it is not required that all this information reaches the parking gateway immediately. It would be acceptable if the information from a parking meter reaches the nearest gateway within a few minutes, say in two minutes. Since a parking meter needs to send approximately 250KB of raw data in two minutes, we need a bit rate of 2083 bits/sec for raw data. However, for wireless communications there is a huge overhead for sending raw data. The actual amount of overhead depends on the specific coding technique used for the wireless communication. For example, for the Rate 1/3 FEC (Forward Error
Correction) coding, three copies of every raw data bit are sent through the air. Thus, for the Rate 1/3 FEC coding the overhead is going to be more than 200%, because some more additional bits will be necessary for packet headers, synchronization bits, end of frames, etc. Similarly, for the Rate 2/3 FEC coding, the overhead is going to be more than 50%. If an overhead of 250% is assumed, each parking meter would send data at rate of 7.29 kilobits/sec to send its warning message along with a picture of the license plate of the violating vehicle. It is very unlikely that under a parking gateway, there would be many parking violations at the same time. If we assume that there are 1000 parking meters under one parking gateway and in the worst case 20% of these meters send warning signals at the same time, then the bandwidth needed by the parking gateway would be approximately 1.458 megabits/sec to accept these messages. A bandwidth of 1.458 megabits/sec can be easily obtained using today’s wireless technology.

Table II: Bandwidth requirement with increase in the % of violations

<table>
<thead>
<tr>
<th>Meters/Parking Gateway</th>
<th>10% of Meters Sending warning messages</th>
<th>15% of meters sending warning messages</th>
<th>20% of meters sending warning messages</th>
<th>25% of meters sending warning messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>300</td>
<td>.218 Mbps</td>
<td>.328 Mbps</td>
<td>.437 Mbps</td>
<td>.546 Mbps</td>
</tr>
<tr>
<td>500</td>
<td>.365 Mbps</td>
<td>.546 Mbps</td>
<td>.729 Mbps</td>
<td>.911 Mbps</td>
</tr>
<tr>
<td>700</td>
<td>.510 Mbps</td>
<td>.765 Mbps</td>
<td>1.020 Mbps</td>
<td>1.275 Mbps</td>
</tr>
<tr>
<td>1000</td>
<td>.729 Mbps</td>
<td>1.093 Mbps</td>
<td>1.458 Mbps</td>
<td>1.822 Mbps</td>
</tr>
</tbody>
</table>
In the graph shown in Figure 22 the bandwidth requirement is shown for various numbers of meters under a gateway.

![Graph indicating increase in required bandwidth with % violations for various numbers of meters under a gateway.](image)

**Figure 22:** Graph indicating increase in required bandwidth with % violations for various numbers of meters under a gateway.

3) Parking Gateway broadcast message to vehicles: Parking Gateway → Vehicles: The PG shall broadcast the messages to the vehicles in its vicinity about the availability of the parking spaces. The data packet contains information about the street name of the parking meters. The 16-bit PID of the parking meter represents this information. The format is shown in Figure 23.

![Data packet format for information on available parking spaces](image)

**Figure 23:** Data packet format for information on available parking spaces
Let’s say each parking gateway has information on N available parking meters in its vicinity, which it extracts from the availability packet sent by the meters. Each broadcast data packet shall be of the following length:

\[ P_1, P_2, \ldots, P_n = N \times 16 \text{ bits} = 16 \times N \text{ bits} \]

Secret key = 128 bit = 16 byte

CRC = 16 bit

SOM and EOM = 16 bits each

Total length = \( 16 \times N + 128 + 16 + 16 + 16 \)

= \( 16 \times N + 176 \) bits

Therefore, \( 16 \times N + 176 \) bits have to be sent over the air for the vehicles in the vicinity of the Parking Gateway to know about the status of parking spaces in that area. For wireless communications, there is a huge overhead for sending raw data. The actual amount of overhead depends on the specific coding technique used for the wireless communication. For example, for the Rate 1/3 FEC (Forward Error Correction) coding, three copies of every raw data bit are sent through the air. Thus, for the Rate 1/3 FEC coding the overhead is going to be more than 200%, because some additional bits will be necessary for packet headers, synchronization bits, end of frames, etc. Similarly, for the Rate 2/3 FEC coding, the overhead is going to be more than 50%. In this thesis work, an overhead of 100% is assumed for the analysis. Let \( B_b \) be the bandwidth required by a PG to broadcast its messages. The value of \( B_b \) can be expressed as:
\[ B_b = \frac{16 \times N + 176}{5000} \text{ Mbps} \]  \hspace{0.5cm} (1)

Table III: Bandwidth requirement for PG with the number of parking meters

<table>
<thead>
<tr>
<th>Number of Meters (N)</th>
<th>Bandwidth required in Mbps ((B_b))</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>0.352</td>
</tr>
<tr>
<td>200</td>
<td>0.672</td>
</tr>
<tr>
<td>400</td>
<td>1.312</td>
</tr>
<tr>
<td>500</td>
<td>1.632</td>
</tr>
<tr>
<td>1000</td>
<td>3.232</td>
</tr>
</tbody>
</table>
The above-calculated values shown in Table III are well within the available bandwidth of DSRC communication range.

As explained in previous Section, the length of the message that has to be broadcasted by the PG is $16\times N +176$ bits. Where $N$ is the number of parking meters under a PG. Consider that the meters are communicating with the PG every $t$ ms. The length of message broadcast by the meter is 65 bits as discussed earlier in Section 4.5. Let $B_p$ be the bandwidth required by a PG to accept messages from the parking meters. If we consider an overhead of 100% in converting the raw bits into wireless packets, then the bandwidth $B_p$ can be expressed as:

$$B_p = \frac{2 \times N \times 65}{1000t} = \frac{130 \times N}{t} \text{ Mbps} \quad \ldots \quad (2)$$
Table IV shows the bandwidth, $B_p$, required by a PG to accept messages from N meters. Table V shows the time required for authentication by a vehicle in $t$ ms.

**Table IV: Bandwidth, $B_p$, required by an PG to accept messages**

<table>
<thead>
<tr>
<th>No of parking meters</th>
<th>Bandwidth, $B_p$, for different values of $t$ (in Mbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$t=10$ ms</td>
</tr>
<tr>
<td>50</td>
<td>0.65</td>
</tr>
<tr>
<td>100</td>
<td>1.30</td>
</tr>
<tr>
<td>200</td>
<td>2.60</td>
</tr>
<tr>
<td>500</td>
<td>6.5</td>
</tr>
</tbody>
</table>

**Figure 23b: Bandwidth $B_p$, required by parking gateway**
Time taken for authentication of a vehicle by a PG is calculated as follows:

Generally it is recommended that a driver should maintain at least a 2-second distance between his vehicle and the vehicle at the front. Let us consider the situation where a driver is maintaining only a 1-second distance instead of a 2-second distance. In this situation the distance maintained between the vehicles is $1.47V$ ft, where $V$ is the velocity of the vehicle in mph. Let $L_v$ be the average length of a vehicle in feet and $R$ be the range of the PG in feet. So there are maximum $\frac{R}{(L_v + 1.47V)}$ vehicles within the range of the PG in each lane. The total number of vehicles under a given PG with $P$ number of roads,

$$N_v = \frac{P \times R}{(L_v + 1.47V)}$$ .................................................. (3)

Let $B_w$ be the total bandwidth available from the wireless communication system, and $B_a$ be the bandwidth available for authentication. The value of $B_a$ can be expressed as:

$$B_a = B_w - (Bp + B_b) \text{ Mbps} .................................................. (4)$$

Let $L_d$ be the length of the digital certificate in bytes. Assuming 100% overhead in converting raw bits into wireless packets, we can say that the time required by each vehicle for authenticating the PG is

$$T = \frac{16 \times L_d}{B_a} \text{ µSec.} .................................................. (5)$$

Total time required for $N_v$ vehicles to authenticate the PG is
\[ T_{nv} = N_v T \ \mu\text{Sec} \]

From Equation 6, the maximum distance a vehicle can travel during the authentication process is given by

\[ D = \frac{1.47 T_{nv} V}{10^6} \ \text{ft} \]

As explained in previous section, the length of the digital certificate is 49 bytes. Figure 25 shows the distance traveled by the vehicle during the authentication process for different ranges of PG. From Table III, the bandwidth \( B_b \) required for PG with 500 meters in its vicinity is 1.632 Mbps. The average length of the vehicle is assumed to be 17 feet and the total bandwidth available from the wireless communication system is assumed to be 9 Mbps, which is same as that of the DSRC systems.

Figure 24 shows the time required for \( N_v \) vehicles to authenticate the PG as a function of the vehicle speed for different communication ranges of the PG. Figure 24 shows that for higher communication range of the PG, more time is needed by the vehicles to authenticate the PG. The reason is that as the range of a PG increases, more vehicles are available with its range. Thus, more time is needed to authenticate the PG by all the vehicles. Figure 24 also shows that when all vehicles are moving slowly, more time is needed for PG authentications. This is due to the fact that when vehicles move slower, the gaps between consecutive vehicles decrease. As a result, there are more vehicles within the range of a PG.
Table V: Time required for authentication by the vehicles

<table>
<thead>
<tr>
<th>Velocity (mph)</th>
<th>Number of vehicles at PG (N)</th>
<th>Bandwidth available for authentication (B_a) mbps</th>
<th>Bandwidth required for broadcast messages by PG (B_b) mbps</th>
<th>Time required for authentication of N=500 vehicles (T_nv) msec</th>
</tr>
</thead>
<tbody>
<tr>
<td>400</td>
<td>50</td>
<td>3.2</td>
<td>1.632</td>
<td>4.168</td>
</tr>
<tr>
<td>400</td>
<td>60</td>
<td>3.2</td>
<td>1.632</td>
<td>4.168</td>
</tr>
<tr>
<td>300</td>
<td>10</td>
<td>3.2</td>
<td>1.632</td>
<td>4.168</td>
</tr>
<tr>
<td>300</td>
<td>30</td>
<td>3.2</td>
<td>1.632</td>
<td>4.168</td>
</tr>
<tr>
<td>300</td>
<td>50</td>
<td>3.2</td>
<td>1.632</td>
<td>4.168</td>
</tr>
<tr>
<td>300</td>
<td>60</td>
<td>3.2</td>
<td>1.632</td>
<td>4.168</td>
</tr>
<tr>
<td>200</td>
<td>30</td>
<td>3.2</td>
<td>1.632</td>
<td>4.168</td>
</tr>
<tr>
<td>200</td>
<td>40</td>
<td>3.2</td>
<td>1.632</td>
<td>4.168</td>
</tr>
</tbody>
</table>
Figure 24: Time required for authenticating a PG by all the vehicles within its range (N=500).

Figure 25 shows the distance that a vehicle will go through while it is authenticating a PG. Figure 26 also shows, the vehicles will move only a fraction of a foot during the PG authentication process. Thus, we can say that the time required for PG authentication by all the vehicles is not too much, and it is acceptable for all practical purposes i.e. the vehicle entering a parking zone shall be able to authenticate a PG within its range.

Figure 25: Distance, a vehicle can travel during a PG authentication process for different ranges of the PG.
Figure 26: Distance, a vehicle can travel during a PG authentication process for different ranges of the PG.

5.2 MEMORY REQUIREMENT

The memory required by the PG to store the information of the parking meters in its vicinity is in the order of Kbytes. To store the information of each parking meter, the PG needs four bytes of memory. Consider there are N meters under a PG’s range. The total memory required by the PG can be expressed as in the number of bytes:
\[ M = \frac{16 \times N + 176}{8} \]

### Table VI: Memory required from a PG

<table>
<thead>
<tr>
<th>Number of Meters (N)</th>
<th>Memory in Kbytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>.222</td>
</tr>
<tr>
<td>200</td>
<td>.422</td>
</tr>
<tr>
<td>400</td>
<td>.822</td>
</tr>
<tr>
<td>500</td>
<td>1.022</td>
</tr>
<tr>
<td>600</td>
<td>1.222</td>
</tr>
<tr>
<td>800</td>
<td>1.622</td>
</tr>
<tr>
<td>1000</td>
<td>2.022</td>
</tr>
</tbody>
</table>

From Table VI it is seen that for 1000 meters under a PG, the maximum memory required by a PG is 2.022 Kbytes. In addition to this memory, additional 100 MB memory is needed by PG to keep the information and for storing the warning messages that include the image file of the license plate of the vehicle and extracting the PID of those meters that are available. This memory also keeps digital certificates and memory to run the program for maintaining the updated information.
Table VII: List of parameters used in the performance analysis

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>Number of meters generating messages</td>
</tr>
<tr>
<td>V</td>
<td>Velocity of the vehicle in Mph</td>
</tr>
<tr>
<td>R</td>
<td>Range of PG in feet’s</td>
</tr>
<tr>
<td>N_v</td>
<td>Number of vehicles under the parking gateway range</td>
</tr>
<tr>
<td>L_v</td>
<td>Average length of the vehicle in feet’s</td>
</tr>
<tr>
<td>B_w</td>
<td>Total bandwidth available</td>
</tr>
<tr>
<td>B_a</td>
<td>Bandwidth available for authentication</td>
</tr>
<tr>
<td>B_b</td>
<td>Bandwidth required for broadcasting messages</td>
</tr>
<tr>
<td>B_p</td>
<td>Bandwidth required by N_v vehicles</td>
</tr>
<tr>
<td>L_d</td>
<td>Length of the digital certificate in bytes</td>
</tr>
<tr>
<td>T</td>
<td>Time required for authentication of one vehicle</td>
</tr>
<tr>
<td>T_nv</td>
<td>Time required for authentication of N_v vehicles</td>
</tr>
<tr>
<td>D</td>
<td>Distance traveled by the vehicle during the authentication</td>
</tr>
<tr>
<td>P</td>
<td>Number of roads around the parking gateway</td>
</tr>
</tbody>
</table>

5.3 COST ANALYSIS

The cost of putting this system in place is minimal, the additional devices that are added to each parking meter is as follows:

a) Two sensors - $10 each = $ 20

b) One low resolution video camera = $10

c) One Bluetooth enabled microprocessor = $25

The total cost for each parking meter is around $50-60, if these devices are bought in wholesale and on a large scale they can come for much lower prices and all the implementation can be done on in $30-35, which is not significant
compared to the ease of use provided to the user and also the increase in the revenue generation.

6. CONCLUSION

In this paper, an architecture for metropolitan area parking and toll collection has been presented. A detailed discussion of the IMPACT architecture and its algorithm has been presented. We have discussed the feasibility of using various sensors for automatic toll collection. The IMPACT system will significantly reduce the operating costs of a metropolitan parking system. Less number of parking officers will be required by a city to manually issue parking tickets. There are still numerous implementation-based issues that we have to study and research.

6.1 FUTURE WORK

For future improvisation a web based registration service can be implemented which shall enable the user to reserve a parking space. Let’s say a user enters a metro area and it gets notification about the available parking space. We can enable some features in our architecture that shall allow the user to reserve a particular parking space before even reaching there. This would help reduce the congestion on the roads because this shall allow the user to reach the parking space directly. Also this system can be improvised for vehicle guidance in which the vehicle is guided to the parking space through this infrastructure.
REFERENCES

[1] Allison L. C. de Cerreño, Ph.D. "The Dynamics of Street Parking in Large Central Cities" NYU, Wagner Rudin Center for Transportation policy & management


http://www.ionet.net/~luttrell/history.html


[5] Tampere Parking Houses Ltd,


Lemminkaisenkatu Finland. Proceedings of the 35th Hawaii International Conference on System Sciences – 2002


http://www.wired.com/news/technology/0,1282,63132,00.html?tw=wn_techhead_1


[14] City of Fort Lauderdale, Florida press release February 12, 2004

[15] VTT Information Technology - A leading edge research institute,

[16] Tekes - Your Contact for Finnish Technology,


[27] N. Asokan, Valtteri Niemi, Kaisa Nyberg,”Man-in-the-Middle in Tunneled Authentication”, Nokia Research Center, Finland


[32] Arthur D Little “Short range radar -automotive applications”

ABSTRACT

AN INTELLIGENT ARCHITECTURE FOR METROPOLITAN PARKING CONTROL AND TOLL COLLECTION

by

Shobhit Shanker
March 2005

Advisor: Dr. Syed Masud Mahmud

Major: Computer Engineering

Degree: Master of Science

U.S Federal and State governments invests millions of dollars for enforcing parking control in the metro city area. Tasks like parking enforcement, towing of illegally parked vehicles, maintenance require many man-hours and resources. The parking control and revenue system in the metro are essentially dependant on devices like coin or token based parking meter, that require the use of exact change and is cumbersome. Also a patrol officer is required to monitor these spaces constantly. This entails the need for a more efficient and redundant system. In this paper an architecture for automated parking meter and driver assistance system that shall be connected to a centralized traffic control authority responsible for parking enforcement and toll collection is proposed. This system would provide a more efficient and redundant way of enforcing parking control and toll collection and also assist drivers in metro area for searching an available parking space. The above-mentioned architecture enables automated parking toll collection.
I received my Bachelors degree in Electronics and telecommunications from Dr Babasaheb Ambedkar Marathwada University, India. I have been working in the area of Intelligent Transportation System (ITS) for the past two and half years under Professor Dr Syed Masud Mahmud at Wayne State University. In a span of 2-3 years as an M.S student I have published papers mainly in the area of intersection collision avoidance and active safety. I formulated and designed various algorithms for the software and hardware architectures in ITS. One of the significant contributions of my thesis work is the development of a full-scale secure protocol for automated parking toll collection and guidance system architectures. This architecture enables critical control and monitoring of parking spaces and an automated toll collection.

Some of my special skills and fields of knowledge include automotive communication networks such as CAN, MOST and J1850.

Starting March 28 I would be working as a software engineer with R & D Technical center at DELPHI AUTOMOTIVE SYSTEMS PRIVATE Ltd, Bangalore, India. Apart from this stuff, I enjoy classical music, reading, playing drums movies, and astronomy.

Publications:
Published and Accepted


Submitted