DESIGN AND ANALYSIS OF A SECURE WIRELESS PROTOCOL FOR ISSUING INTERSECTION COLLISION WARNINGS

by

SRINIVAS R MOSRA

THESIS

Submitted to the Graduate School of Wayne State University, Detroit, Michigan

in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

2004

MAJOR: COMPUTER ENGINEERING

Approved by:

Syed Masud Mahmud             Dec. 13, 2004
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 virtues. This research work could not have been accomplished without his constant guidance. I also thank my thesis committee members Dr. Pepe Siy and Dr. Qiang Cheng 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 ........................................................................................................... i

LIST OF TABLES .................................................................................................................. v

LIST OF FIGURES ................................................................................................................ vi

1 INTRODUCTION .................................................................................................................. 1

2 LITERATURE REVIEW ....................................................................................................... 5

   2.1 COLLISION AVOIDANCE ............................................................................................... 7
       2.1.1 Collision Avoidance System ............................................................................... 7
       2.1.2 Levels of Warning ................................................................................................. 8
       2.1.3 Rural Intersection Collision Avoidance ................................................................. 8
       2.1.4 BATTELLE Intersection Collision Avoidance System ........................................... 9
       2.1.5 Driver Safety Support Systems for Intersection Collision Prevention .......... 10

   2.2 WIRELESS COMMUNICATION .................................................................................. 10
       2.2.1 Dedicated Short Range Communications (DSRC) .............................................. 10
       2.2.2 Secure Inter-Vehicle Communication ................................................................ 11
       2.2.3 Secure Wireless Communication ...................................................................... 12

   2.3 SECURITY TECHNIQUES ............................................................................................ 13
       2.3.1 Digital Certificates ............................................................................................... 13
       2.3.2 Key and Certificate Management ........................................................................ 14
       2.3.3 Trusted Third Parties and Cross Certification ..................................................... 15

3 METHODOLOGY ................................................................................................................. 17

   3.1 PROPOSED TECHNIQUES FOR ROAD NUMBER, LANE NUMBER AND
       DISTANCE FROM THE INTERSECTION DETECTION SYSTEM .................. 20
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.1</td>
<td>Barcode System</td>
<td>20</td>
</tr>
<tr>
<td>3.1.2</td>
<td>RF Method</td>
<td>21</td>
</tr>
<tr>
<td>3.1.3</td>
<td>Magnetic Strips</td>
<td>21</td>
</tr>
<tr>
<td>3.2</td>
<td>SECURED INTERSECTION TRAFFIC CONTROLLER (ITC) AND WIRELESS PROTOCOL</td>
<td>22</td>
</tr>
<tr>
<td>3.2.1</td>
<td>ITC Protocol</td>
<td>22</td>
</tr>
<tr>
<td>3.2.2</td>
<td>Digital Certificate Format</td>
<td>25</td>
</tr>
<tr>
<td>3.3</td>
<td>ITC VALIDATION</td>
<td>27</td>
</tr>
<tr>
<td>4</td>
<td>PERFORMANCE ANALYSIS</td>
<td>32</td>
</tr>
<tr>
<td>4.1</td>
<td>BANDWIDTH REQUIREMENT</td>
<td>32</td>
</tr>
<tr>
<td>4.2</td>
<td>MINIMUM REQUIRED RANGE OF AN ITC</td>
<td>39</td>
</tr>
<tr>
<td>4.3</td>
<td>MEMORY REQUIREMENT</td>
<td>41</td>
</tr>
<tr>
<td>5</td>
<td>CONCLUSION</td>
<td>44</td>
</tr>
<tr>
<td>6</td>
<td>FUTURE WORK</td>
<td>45</td>
</tr>
<tr>
<td>REFERENCES</td>
<td></td>
<td>46</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td></td>
<td>Error! Bookmark not defined.</td>
</tr>
<tr>
<td>AUTOBIOGRAPHICAL STATEMENT</td>
<td></td>
<td>54</td>
</tr>
</tbody>
</table>
LIST OF TABLES

Table 1: Key 2002 National Highway and Traffic Administration (NHTSA) Statistics................................................................. 5

Table 2: Bandwidth, $B_b$, required for an ITC to broadcast its messages ............ 33

Table 3: Bandwidth, $B_v$, required by an ITC to accept messages from $N_v$ vehicles. .......................................................................................................................... 34

Table 4: Distance traveled by the vehicles in $t$ ms. ................................................. 34

Table 5: Maximum distance traveled by a vehicle during authentication process
(N=4, Ln=4, S=3) ........................................................................................................ 37

Table 6: Distance traveled by a vehicle before it stops with a deceleration of 20
ft/sec$^2$ .......................................................................................................................... 40

Table 7: Distance traveled by a vehicle before it stops with a deceleration of 15
ft/sec$^2$ .......................................................................................................................... 40

Table 8: Memory required from an ITC ................................................................. 42

Table 9: List of parameters used in the performance analysis............................... 43
LIST OF FIGURES

Figure 1: Version 3 public key certificate ................................................................. 15
Figure 2: Sample certification hierarchy ................................................................. 16
Figure 3: Tasks performed by the Intersection Traffic Controller (ITC) ............... 18
Figure 4: Tasks performed by the vehicle’s on board computer ......................... 19
Figure 5: An overview of the ITC message format ............................................... 23
Figure 6: Format of the vehicle to ITC message .................................................. 25
Figure 7: Format of the digital certificate ............................................................... 26
Figure 8: Certificate chain ...................................................................................... 27
Figure 9: Process of obtaining the public key and verification of ITC ................. 28
Figure 10: Process of obtaining the public key and verification of ITC (Contd.) .. 29
Figure 11: Hierarchy of certificate authorities ....................................................... 31
Figure 12: Time required for authenticating an ITC by all the vehicles within its range (for N=4 and L_n=4) ................................................................. 37
Figure 13: The distance, a vehicle can travel during an ITC authentication process for different ranges of the ITC (for N=4 and L_n=4) ....................... 38
Figure 14: The distance, a vehicle can travel during an ITC authentication process for different ranges of the ITC (for N=8 and L_n=8) ............... 39
1 INTRODUCTION

There have been major improvements in vehicle safety since the 1960’s. The introduction of safety features such as seat belts, air bags, crash zone, lighting and new vehicle structures dramatically reduced the rate of crashes, injuries and fatalities. The fatality rate per hundred million miles traveled has fallen from 5.5 to 1.7 in the period from mid-1960s to 1994 [1]. However, in spite of these impressive improvements, according to NHTSA each year in the United States, motor vehicle crashes still account for a staggering 40,000 deaths, more than three million injuries, and over $130 billion in financial losses. All of these safety features are either static or passive. They act to minimize collision damage or give the driver visual assistance or warning at specific geographic areas.

In order to reduce the number of traffic accidents and improve the safety and efficiency of traffic, the research on Intelligent Transportation System (ITS) has been developed for many years in many countries [2]. With recent advance in sensing, computing, and communication technologies, new driving assistance systems such as night vision and collision warning systems (CWS) have been designed, tested, and deployed [1, 3, 4, 5, 6]. While night vision systems simply provide visual assistance to drivers in dark environment, collision warning and avoidance systems generally exhibit some intelligence. Despite the fact that intersection collision accounts for almost 30% of all crashes, intersection collision avoidance systems received less attention than the forward collision avoidance systems [4, 7]. The reason, besides the fact that the intersection collision problem is more complicated than rear-end crash, is the limitation of the radar
technology, the most widely used object sensing method in vehicle collision avoidance systems. Most radar systems require line-of-sight for object detection. This renders ineffective collision warning/avoidance system that requires line-of-sight for threat detection.

The present technologies that are being investigated to avoid intersection collisions are differential global positioning systems (DGPS), electronic compasses, roadside sensors, etc. There are several disadvantages of these technologies. For example, the GPS signals have some errors and in some areas, especially in downtown areas with very tall buildings, the signals may not be detected. The roadside sensors may not detect some vehicles if there are multiple lanes on the road.

This thesis work presents an intelligent architecture for issuing intersection collision warnings using wireless communications. It becomes imperative that the vehicles exchange dynamic information such as speed, acceleration, position and direction in real time. Wireless communications do not require line-of-sight. Thus, using wireless communication technologies, the vehicles can inform each other about how far they are from the intersection and receive the dynamic information of the signal lights and the status of the intersection. The goal of the Intersection Automotive Collision Avoidance Systems (IACAS) is to detect and warn the driver of potential hazard conditions. Therefore, it is of extreme importance that the data integrity should be taken care of, which means that the system should be immune to security attacks. It should be ensured that all communication between various vehicles is done in a secure fashion. Otherwise,
a person with malicious intent might inject incorrect information into the wireless links leading to a disaster, not only for the individual himself/herself but also for the hundreds of others, which are around him/her on the road. The loss of confidentiality and integrity and the threat of denial of service (DoS) attacks are risks typically associated with wireless communications. Many current communications protocols and commercial products provide inadequate protection and thus present unacceptable risks for any operations [8]

For the Intersection traffic controller to communicate securely with the vehicles near the intersection, it is necessary that they share some kind of secret key(s). In Client-Server based architecture this is done by the server using protocols such as SSL, VPN tunneling [9], etc. Ronald Miller and Qingfeng Huang have done some work in the area of Automotive Collision Avoidance Systems (ACAS) using wireless communication technologies [10]. But their systems are not secure, and can easily be attacked by hackers. In our architecture, security aspects such as authentication, authorization, and data integrity have been implemented using public-key infrastructure (PKI).

In the proposed technique, an Intersection Traffic Controller (ITC) is installed at the intersection that broadcasts the status of the intersection and communicates with the vehicles approaching the intersection. Vehicles cooperatively share the critical information with the ITC for collision anticipation, i.e., location, velocity, acceleration, etc and achieve threat detections. The location of the vehicle is determined by using a sensor in the vehicle and some devices embedded in the road system. The embedded devices may be magnetic strips, a barcode or RF
transmitters. By sharing the information between vehicles and the ITC, each vehicle is able to predict potential hazard. The IACAS requires minor support infrastructure.

The rest of the work is organized as follows. Chapter 2 presents the literature review, including the previous work done on the intersection collision avoidance system. Chapter 3 presents the proposed technique for Issuing Intersection Collision Warnings along with the proposed techniques for determining Road number, Lane number, distance from intersection and proposed security techniques. Chapter 4 presents performance analysis, in terms of protocol, bandwidth and memory size, for the proposed technique. Chapter 5 presents the conclusions and Chapter 6 presents future work.
Many different aspects need to be considered when attempting to determine the architecture for implementing intersection collision avoidance systems (ICAS). Justification for such a study comes from the facts that show that there is a need to design a system that could decrease the number of collisions between vehicles at intersections.

Table 1: Key 2002 National Highway and Traffic Administration (NHTSA) Statistics

<table>
<thead>
<tr>
<th>Category</th>
<th>Number</th>
<th>Percentage</th>
<th>Societal cost in Billion $</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total fatality crashes</td>
<td>38,409</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total intersection-related fatality crashes</td>
<td>8,760</td>
<td>22.8</td>
<td>22</td>
</tr>
<tr>
<td>Total injury crashes</td>
<td>1,929,000</td>
<td>55.3</td>
<td>69</td>
</tr>
<tr>
<td>Total intersection-related injury crashes</td>
<td>1,066,000</td>
<td>55.3</td>
<td>69</td>
</tr>
<tr>
<td>Total property-damage-only (PDO) crashes</td>
<td>4,348,000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total PDO intersection-related crashes</td>
<td>2,092,000</td>
<td>48.1</td>
<td>5</td>
</tr>
<tr>
<td>All crashes</td>
<td>6,316,000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total intersection-related crashes</td>
<td>317,000</td>
<td>50.2</td>
<td>96</td>
</tr>
<tr>
<td>Total Fatalities</td>
<td>42,815</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fatalities at intersections</td>
<td>9,612</td>
<td>22.4</td>
<td></td>
</tr>
</tbody>
</table>

In 2002 approximately 6.3 million crashes occurred out of which 3.2 million crashes are related to intersection collisions, representing 50 percent of all reported crashes. 9,612 fatalities (22 percent of total fatalities) occurred at or
within an intersection environment. The cost to society for intersection crashes is approximately $96 billion a year [11]. Table 1 shows the crashes occurred in 2002.

Crash Statistics data, collected by the NHTSA (National Highway Traffic Safety Administration) show that 88% of rear end collisions are caused by driver inattention and following too closely [1]. Streff [12] listed unsafe driving acts and the percentage of collisions caused by each act. It was found that failure-to-yield caused 19.3% of collisions, speeding caused 16.9%, following too close caused 10.3%, driver inattention caused 6.6%, careless driving caused 5.8%, and other driver behavior accounted for 17.9%, the rest were spread across 13 other categories. Therefore, it is assumed that the collisions caused by inattention, following too close, and careless driving could be combated through the use of Collision Avoidance Systems (CAS), thereby reducing the number of collisions by up to 22.7%.

These numbers show that much pain and suffering occurs from vehicular accidents, particularly at intersections. There is an obvious need to decrease these numbers. The ideal solution for this problem is the implementation of new technologies to reduce the number of collisions.

The new vision for intelligent transportation system is based on information management and availability, connectivity and system control and optimization – in short, the creation of an integrated national network of transportation information. The information to be gathered, managed and distributed includes real-time information on the physical state of the infrastructure, how it is being
built, used, maintained and kept secure. Some of the previous work and key entities of Intelligent Transportation System (ITS) are mentioned here briefly.

2.1 COLLISION AVOIDANCE

2.1.1 Collision Avoidance System

A collision avoidance system (CAS) is a system that alerts a driver to a probable collision situation [13]. These systems use a combination of object detection sensors and existing electronic systems to determine if a collision is probable. A CAS typically will contain three subsystems: recognition, processing, and presentation [14]. The activities of these subsystems include recognizing data involving potential collisions, processing this data into a usable format for the driver, and presenting the data to the driver in a usable structure. The main purpose of a CAS is to warn the driver of a hazardous situation that requires the immediate attention of the driver in order to avoid a collision with another vehicle or object. The system is also able to reduce the emergency braking response time of the driver, and therefore aid in collision avoidance. The driver would also receive feedback from the system about situations that may become hazardous. This knowledge should help the driver prevent similar occurrences in the future [15]. A CAS is not intended to provide the driver with continuous information about traffic flow, which would cause the driver to constantly monitor the system. Instead, it alerts the driver to an error or other potential hazardous behavior, such as improperly directed attention, misjudgment, or drowsiness [16]. Some of the proposed systems also use inter-vehicle communications to exchange dynamic information about each other and make crash avoiding maneuvers [17].
2.1.2 Levels of Warning

Many researchers have stated the need for at least two levels of alarm when implementing a CAS into a vehicle [14, 15, 18]. The system should produce at least two levels of warnings: imminent and cautionary warnings. An imminent warning should be activated when immediate evasive actions are immediately needed to avoid a collision. A cautionary warning should be initiated when there is a possibility of a collision and the driver needs to be alerted, but in which the driver does not need to take immediate evasive action. The alarm activation is preferred when there is danger of colliding with an obstacle, and should remain inactive if the driver could brake normally [19]. One problem with cautionary warnings is that they are activated more often than imminent warnings, which can potentially annoy the driver and cause him/her to ignore the warning [20]. This is especially true when the driver’s attention is directed to the roadway. Thus, the driver may tend to ignore the warnings, resulting in nuisance alarms.

2.1.3 Rural Intersection Collision Avoidance

Accidents caused by drivers who fail to stop, or fail to yield the right-of-way to cross traffic after stopping, are becoming increasingly frequent at some rural intersections on the state highway system. Due to the relatively high speed of the cross traffic, accidents caused by failure to stop or failure to yield the right-of-way can be severe. These accidents continue to occur even though the traffic control devices in place at rural highway intersections meet or exceed the requirements set forth in the Manual on Uniform Traffic Control Devices (MUTCD).
Rural Intersection Decision Support (IDS) [21] is built on recent advances in intelligent transportation systems (ITS) technology to address a significant public safety problem. IDS use a suite of advanced traffic monitoring and communication technologies, to track vehicles approaching the intersection. Human-factors and cognitive psychology are used to design and evaluate ways of communicating relevant information to the driver waiting to cross.

The focus is on driver error at rural intersection crashes, which involve a driver on a minor roadway failing to select a proper gap in the traffic stream when trying to cross a high-speed, high-volume highway at a through/stop intersection. This problem was identified by the unsignaled intersection panel of National Cooperative Highway Research Program (NCHRP) Study, which developed guidelines for the implementation of the American Association of State Highway and Transportation Officials (AASHTO) Strategic Highway Safety Plan [22]. The report specifically suggests that a strategy be developed to “Provide an Automated Real-Time System to Inform Drivers of the Suitability of Available Gaps for Making Turning and Crossing Maneuvers.”

2.1.4 BATTELLE Intersection Collision Avoidance System

Battelle [23] is supporting a federal project to develop specifications for a system that would help drivers avoid intersection collisions. The goal of the project is to develop a system that will alert drivers to a potential crash situation as they approach an intersection. Or, if necessary, the system can assume control of a vehicle if the driver is unable to respond in time.
The equipment in the vehicle could include sensors of several varieties - microwave, laser, radar, or video imaging systems - as well as computers and communications equipment. Potential infrastructure equipment might include intersection surveillance sensors and road-to-vehicle transponders. These systems consider such parameters as velocity, heading, acceleration of the subject vehicle, presence/configuration of the traffic light, signal light phasing, and the dynamic state of other vehicles in the vicinity of the intersection.

2.1.5 Driver Safety Support Systems for Intersection Collision Prevention

This system [24] aims to prevent collision at intersections without signal lights and without clear view ahead. This system also provides a mechanism for issuing a message to the vehicle about the condition of the signals whether they are about to turn red, so that the driver does not speeds up in order to cross the intersection at the yellow light. It essentially uses image detectors to detect the approaching vehicles and infrared beacons to transmit this information to the vehicles. Warning messages are given to the vehicle’s embedded unit that will have wireless capabilities. Such systems have the limitation of weather, because in cases of snow or heavy rain, the control unit might get an error message or false signal from the camera.

2.2 WIRELESS COMMUNICATION

2.2.1 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) allows high-speed communications between vehicles and the roadside, or between vehicles, for ITS; it has a range of up to 1,000 meters [25]. 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
- Highway-Rail intersection warning.

In our earlier work, a technique for secure inter-vehicle communication was developed [17]. A brief description of our earlier work is presented in the following subsection to make the readers familiar with the technique for developing a secure inter-vehicle network.

**2.2.2 Secure Inter-Vehicle Communication**

To build a secure inter-vehicle wireless network, every vehicle must be equipped with a wireless device to communicate with the neighboring vehicles as well as with the Intelligent Transportation Towers (ITTs). An ITT will be responsible for
authenticating the vehicles when the vehicles will come within the range of the ITT. An intelligent vehicle will have three different types of wireless links: 1) a link for the in-vehicle wireless network, 2) a link for inter-vehicle wireless network, and 3) another link for the vehicle to ITT communications. When a vehicle is manufactured, at that time a wireless device will be installed in it. At the time of installing the wireless device, a set of keys will be given to the device. A copy of these keys will also be kept in a secure central server. Different vehicles will be given different sets of keys. These keys will be securely kept in the central server. If the secure central server of a particular vehicle is going to be maintained by the manufacturer of that vehicle, then every auto company will have its own central server. Authorized organizations will be able to access the keys of a vehicle by using the vehicle’s ID (VID) number. If the auto companies maintain the central servers, then the VID of a vehicle will indicate which server to go to for accessing the keys.

2.2.3 Secure Wireless Communication

Intersection collision avoidance systems that use wireless communication technology must be protected from various types of security attacks. Securing any type of communication links involves three key requirements. First, the links must be protected from eavesdropping, so that unauthorized persons can’t access private information. Second, the end users must be authenticated before anything is sent to or received from them. Third, the communication links must be protected from tampering by hackers. If all information is transmitted in encrypted form, then that should protect the communication links from eavesdropping. If
standard techniques such as, Cyclic Redundancy Check (CRC) [26, 27] Check Sum [27], Hamming Code [28], etc. are used with the information, before the information is encrypted, then that should protect the links from tampering. But, the most vital task in establishing a secure communication link is the authentication of the parties on both sides of the communication link and exchanging their encryption keys.

Digital identities and security technologies enable the security services like authentication, authorization, digital signature and encryption to exchange messages over the wireless network. A brief background of security techniques is presented in the following subsections.

2.3 SECURITY TECHNIQUES

2.3.1 Digital Certificates

There is a broad range of applications for digital certificates: electronic banking, electronic payment systems, e-mail communication, identification in communication with public authorities (e.g. transportation, tax declaration, court documents, electronic passports, public health service, etc.), electronic contracts, selective web access, selective database access, etc.

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 [29, 30]). 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 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.

2.3.2 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) that issued the certificate and the certificate validity period. Figure 1 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.
The certification of identity is only the simplest form of a certificate. Similar extensions are provided with role-based systems as the Simple Public Key Infrastructure (SPKI) [31]. With the use of application-specific extensions, the function of the certification authority is extended to the verification of the respective attributes of the certificate holders.

### 2.3.3 Trusted Third Parties and Cross Certification

The Nation-wide use of certificates causes the emerging of a large number of certificate issuers. One cause for this is that a certificate issuer needs a certain regional presence in order to verify the identity of a person. From this point of view, an organization issuing certificates consists of a large number of locally operating entities, independent from each other. For the end users, the management of different trustworthy public keys is not applicable, because each of these would have to be transmitted in a secure way. This problem can be solved by the use of cross certificates [32]. These are certificates issued by a CA certifying another CA. In this way, an end user is able to verify a certificate issued by a CA whose public key was not directly transmitted to the end user.
For the verification, there must only be a link via cross certificates to the CA whose trustworthy public key is with the end user. This link is also called certification path or chain of trust. The CA whose trustworthy public key is provided is called trusted third party [33]. Using these mechanisms, a system can be built that consists of several certification authorities issuing certificates for individuals but also building links between each other using cross certificates. In an ideal situation, each end user is able to verify the certificates of any other person using only one trusted third party in this system. The combination of certification authorities linked to each other via cross certificates and the end users is called public-key infrastructure [34]. Figure 2 shows a sample certification hierarchy.
3 METHODOLOGY

This section of the thesis work presents a technique for issuing intersection collision warnings. This technique requires that every vehicle must be equipped with a wireless device to communicate with the Intersection Traffic Controller (ITCs). Here it is assumed that all intersections are installed with an ITC, and all roads of the intersection are equipped with a mechanism through which the vehicle’s on-board computer can determine the road number and lane number on which the vehicle is present and the distance from the intersection as mentioned in the subsequent Section 3.1. It is also assumed that all vehicles are equipped with the sensors, which are capable of detecting the road number, and lane number on which the vehicle is present and distance from the intersection. The ITC broadcasts the condition of the intersection using messages. A message contains all the dynamic information of the intersection. For example, the message indicates how soon the traffic light will change from its current state to the next state, whether the vehicle can take a left turn, whether any vehicle has violated the traffic signal, etc.

The ITC broadcasts the message continuously and receives the information from the vehicles approaching towards the intersection. The information received from the vehicles contains the vehicle’s speed, acceleration and distance from the intersection. From vehicles information, ITC calculates whether the vehicle can cross the intersection without violating the signal. If the vehicle violates the signal, ITC sets the violation bit in the broadcasting message. Figure 3 shows the functions performed by the ITC.
As the vehicle approaches an intersection, using the infrastructure system present at the intersection the vehicle’s onboard computer knows on which road number, lane number it is present and the distance from the intersection. The vehicle receives its speed and acceleration from the in-vehicle network. This information is sent to the ITC through wireless communication protocol using specific message format as shown in the Figure (6).
Start

Get the road number, lane number and distance from the Intersection

Receive the message from the ITC of the intersection

Check for the message to get information about the corresponding road and lane number.

Check for the signal

Is it Green?

Yes

Check for the time when it turns to red

No

Calculate the distance between the vehicle and the intersection

Is it Yellow?

Yes

Can the vehicle cross the intersection before the signal changes to red?

No

Has any vehicle violated the rule?

Yes

You are fine

End

No

Stop the vehicle

Figure 4: Tasks performed by the vehicle’s on board computer
The vehicle’s onboard computer receives the broadcasted messages from the ITC and checks the information in the message that corresponds to the road number and lane number of the vehicle.

From the message, the vehicle’s on board computer determines whether the signal at the intersection is green, yellow or red and the time left for the signal to change from its current state to the state. The on board computer calculates the time left for the vehicle to reach the intersection and checks whether the vehicle can pass the intersection without violating the traffic signal. From the message, the vehicle’s on board computer knows if any other vehicle has violated the traffic signal. If any vehicle violates the traffic signal, the on board computer issues pre warning to the driver indicating that a vehicle has violated the traffic signal. Figure 4 shows the algorithm executed by the onboard computer of a vehicle for issuing the intersection collision warning.

3.1 PROPOSED TECHNIQUES FOR ROAD NUMBER, LANE NUMBER AND DISTANCE FROM THE INTERSECTION DETECTION SYSTEM

In the proposed architecture, it is assumed that every road at an intersection has an embedded mechanism that carries information like the road number, lane number and the distance from the intersection. The following subsections show a brief description of the techniques that can be used to design the embedded mechanism.

3.1.1 Barcode System

In this technique, a barcode is put on the road using paint. Each lane in the road would be bar-coded and would contain information such as road number and
lane number. The bar code will also indicate its distance from the intersection. The bar-code technique will require that each vehicle have a light source embedded in its chassis. The disadvantage of this system is that in snow, heavy rain or dust the system might behave erroneously.

### 3.1.2 RF Method

In this technique, four to five low power very short range Radio Frequency (RF) transmitters are used. These devices would be embedded in the road. The devices would be located sequentially one after another on the road in order for them to create a very narrow band of electromagnetic field. Each of these devices will transmit at frequency $F$ and each lane in the road would have an array of such transmitters at a unique frequency, say $F_1$, $F_2$, $F_3$, and $F_4$ for lane 1, 2, 3 and 4, respectively. As soon as a vehicle comes in the range of these devices, the vehicle would detect a narrow beam of signal and accept the information from the strongest signal and ignore the other lower strength signals. The message contained in this signal is for that particular lane on which the vehicle is moving. From the messages, the vehicle will knows the road number, lane number and its distance from the intersection.

### 3.1.3 Magnetic Strips

Each road has multiple sets of magnetic strips placed at some predefined distances from the intersection. These sets of strips are arranged in such a way that they carry information like distance from the intersection, road number and lane number. The first two strips carry the road number information and the next two strips carry the information of distance from the intersection. The last four
strips carry the lane number information. By sensing the fields of the magnetic strips, the magnetic sensor of a vehicle detects where the vehicle is with respect to road number, lane number and distance from the intersection. When a vehicle passes over the strips, the vehicle’s sensor detects a positive pulse when it goes over a magnetic strip with positive voltage and a negative pulse when it goes over a magnetic strip with negative voltage. The bit coding for a positive pulse is one and for a negative pulse is zero.

3.2 SECURED INTERSECTION TRAFFIC CONTROLLER (ITC) AND WIRELESS PROTOCOL

This section of the thesis work explains the protocol for the ITC that has to be broadcasted and the protocol for the digital certificates.

3.2.1 ITC Protocol

The role of ITC in the Intersection Collision Avoidance System (ICAS) is to broadcast the condition of the intersection for the traffic crossing the intersection [11]. The broadcasted messages have a specific format so that all the vehicles can understand easily. The length of the message varies depending upon the number of roads, lanes and signal lights present at an intersection. The messages are broadcasted in the form of packets. Figure 5 shows an overview of the message format that is broadcasted by an ITC.

All messages begin with a Start of Message (SOM) field. This serves to identify the beginning of a message. The second field in the message is always the ITC field, which contains 16-bit ITC number field. This field is used to identify the intersection. The third field in the message is the vehicle violation field. This field
contains one bit, which is used to determine whether any vehicle has violated the traffic signal.

Field number four is called the Intersection status field. This is a variable length field. The first four bits are used to specify the number of roads present at the intersection. Following these four bits are road information fields. The length of road information fields depends upon the number of roads present at the intersection.

<table>
<thead>
<tr>
<th>SOM</th>
<th>ITC Number Field</th>
<th>Vehicle Violation Field</th>
<th>Intersection Status Field</th>
<th>CRC Check</th>
<th>EOM</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Number of Roads At Intersection (N)</td>
<td>Road 1 Information Field</td>
<td>Road 2 Information Field</td>
<td>. . . .</td>
<td>Road N Information Field</td>
</tr>
<tr>
<td></td>
<td>Road Number</td>
<td>Road Status Field</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Number of Lanes</td>
<td>Number of Signal Lights</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lane Information Field (LIF)</td>
<td>Lane Information Field (LIF)</td>
<td>Lane Information Field (LIF)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Number of Lanes Following a Particular Signal Light (P)</td>
<td>Lane Numbers</td>
<td>Lane Status Field</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lane Numbers</td>
<td>Signal Status Field</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 5: An overview of the ITC message format.
The road information field is again divided into a 4-bit road number field and a road status field. The length of the road status field depends upon the number of signal lights and lanes present on a particular road. The first part of the road status field is the number of lanes field, which is four-bit wide. This field specifies the number of lanes present on a particular road. The second field is the number of signal lights field, which contains two bits. This field specifies the number of signal lights present for a particular road. Following the number of signal lights field is the lane information field. The lane information field is of variable length. This field is repeated depending upon the number of signal lights present on a road.

The lane information field is divided into four sub fields. The first sub field contains four bits. This field specifies the number of lanes following a particular signal light. The second sub field specifies the lane numbers of the road following the respective signal light. The third sub field is lane status field, which contains four bits. These four bits are L bit, T bit, R bit and U bit, which specify whether the vehicles on a particular lane can go left, through, right or make a U turn, respectively or not. The last sub field is the signal status field, which has two fields. The First field is the signal field which is of three bits and specifies the signal status i.e. whether the signal is red, green, yellow, blinking yellow or blinking red and the second field is the time field which contains 31 bits, specifying the time left for the signal change.

Following the Intersection status field is the CRC field. It consists of 16-bit Cyclic Redundancy Check code, which allows the receivers to verify the correctness of
the received message. The final field of the message is the End of Message (EOM) field, which serves as the end of the message.

<table>
<thead>
<tr>
<th>SOM</th>
<th>Vehicle road number</th>
<th>Velocity</th>
<th>Acceleration</th>
<th>Distance from the intersection</th>
<th>CRC</th>
<th>EOM</th>
</tr>
</thead>
</table>

Figure 6: Format of the vehicle to ITC message

Figure 6 shows the format of the message that is to be received by the ITC from the vehicles approaching towards the intersection. The first field is the Start of Message (SOM) field, which serves to identify the beginning of a message. The second field is of four bits specifying the road number of the vehicle. The third field contains 12 bits, and it specifies the velocity of the vehicle. The fourth field contains 16 bits, and it specifies the acceleration of the vehicle. Following the acceleration field is the Distance field, which has 16 bits to specify the distance from the intersection. The next field is the CRC field. It consists of a 16-bit Cyclic Redundancy Check code, which allows the ITC to verify the correctness of the received message. The last field is the End of Message (EOM) field. The total length of the message that has to be broadcasted by the vehicle is 96 bits.

3.2.2 Digital Certificate Format

The secured system is based on digital signatures. A digital signature is a kind of cryptographic check sum where the vehicle’s On Board Unit (OBU) can verify the checksum and thus convince itself that the messages it received is the one that was sent by an authorized ITC.

Digital certificates not only carry the public key but also some information about what it’s authorized to do. In the present system, OBUs (the units in cars) contain
only public key and a range of valid dates. The public key is issued to the OBU by USDOT at the time of manufacturing the vehicle. ITC's, on the other hand contain their public key, unique serial number, valid dates and digital signature.

Figure 7 shows the format of the digital certificate.

<table>
<thead>
<tr>
<th>SOM</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 7: Format of the digital certificate

The digital certificate contains nine fields. The first field is Start of Message (SOM) field, which contains 16bits and is used to identify the beginning of the certificate. The second field is the hierarchy level field, which is one byte long. The lower 3 bits specify the hierarchy level and the remaining bits are reserved for the future use. The third field is the Issuer ID field. This field serves to identify which Certificate Authority (CA) is signing the certificate. The length of this field is three bytes. Field number four is validity field. This field specifies how long the certificate is valid and is four bytes long. The fifth field is Subject ID field, which is three bytes long. This field specifies the ID of the certificate recipient. Field number six is called Public Key field. This field is 16 bytes long and is used to determine the public key of the certificate recipient. Seventh field is the Digital signature field with 16 bytes. This field is used to verify the signature signed by the certificate issuing authority. Next field is the CRC field, which is two bytes long and is used to verify the CRC check. The last field is the End of Message (EOM) field and is served to specify the end of message with two bytes length. The total length of the digital certificate is 49 bytes.
3.3 ITC VALIDATION

In the architecture, unidirectional chain of certificates are used for validating the ITC messages in which USDOT 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. Each state acts as a certifying authority and signs a certificate for each county. 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 ITC. An ITC is issued a key pair (private, public) by its city. This key pair is embedded in the hardware of the ITC. For an ITC the certificate chain looks like the one shown in Figure 8.

Figure 8: Certificate chain.
Start

Is the vehicle in the range of ITC?

Yes

Request the ITC for its State certificate & check the validity of the certificate

No

Is the certificate valid?

Yes

Extract the Public key of state

Request the ITC for its County certificate & check the validity of the certificate

No

Is the certificate valid?

Yes

Extract the Public key of County

No

Figure 9: Process of obtaining the public key and verification of ITC
Figure 10: Process of obtaining the public key and verification of ITC (Contd.)

The ITC broadcasts all traffic-related messages after encrypting the messages by its private key. All vehicles that are near the intersection need the public key
of the ITC to decrypt the messages sent by the ITC. The vehicles can get the
public key of the ITC by going through the chain of certificates that are
embedded in the ITC. As a vehicle approaches the intersection it starts receiving
the messages from the ITC. The vehicle’s OBU ignores the messages it received
until the OBU receives the public key of the ITC. To get the public key of the ITC
the OBU first requests the ITC for the state certificate. From the state certificate
sent by the ITC the OBU verifies the signature using the USDOT’s public key,
which is embedded in its software and extracts the public key of the state. After
extracting the public key of the state, the OBU requests the ITC for the county
certificate. Using the state’s public key it verifies the county certificate and gets
the public key of the county. Next the OBU asks for the city certificate and
verifies the certificate using the count’s public key and extracts the city’s public
key from the certificate. Finally the OBU requests for the ITC certificate and using
the city’s public key it verifies the ITC certificate and extracts the public key of the
ITC. Once the OBU gets the public key of the ITC, it starts accepting the
messages received from the ITC. The whole process of verification is explained
in brief using Figure 9 and Figure 10.

Let’s examine a simple example. Figure 11 illustrates the hierarchy of CAs. The
hexagons represent the CAs, the arrows represent certificate issuance, and the
sectional rectangles represent certificates. Consider an ITC, which is at the
intersection of Warren and Woodward roads, is broadcasting the status of the
intersection and a vehicle V1 is approaching the intersection and attempting to
verify the ITC certificate.
We construct a certification path between the ITC certificate and the US-DOT certificate. The certification starts from the US-DOT certificate and works its way to the ITC. The path is US-DOT → Michigan-DOT → Wayne-DOT → Detroit-DOT → ITC. The vehicle’s OBU verifies the Michigan-DOT certificate and confirms that US-DOT is the issuer of Michigan-DOT certificate and hence trusts the Michigan-DOT. Similarly the vehicle’s OBU verifies the certificate of Wayne-DOT and confirms that Michigan-DOT is the issuer of Wayne-DOT certificate and so on until the ITC certificate is verified.
4 PERFORMANCE ANALYSIS

An ITC will have to broadcast (in real time) the information of the approaching vehicles and change of traffic signals to all the vehicles approaching towards the intersection. The ITC has to broadcast the message once in every 10 milliseconds so that the vehicles receive the updated signal information and keep track of the situation at the intersection. Let us assume that a particular intersection has N number of roads with Ln lanes per road heading towards the intersection and each road has S signal lights. Each signal light requires 42 bits and each lane requires 4 bits to specify the lane number. Four bits are required to mention road number and six bits are required to mention the number of lanes and signal lights present on a road. The number of bits required to specify the information of one road is \((42S + 4L_n + 10)\) bits. To specify the information of N roads, the number of bits required by the intersection status field is \(N(42S + 4L_n + 10)\). The SOM and EOM field requires 32 bits. ITC field requires 20 bits. The violated vehicle information field requires one bit. The CRC field requires 16 bits. Apart from the intersection status field, we require additional 69 bits. The total length of the message that is to be broadcasted by the ITC is \(N(42S + 4L_n + 10) + 69\).

4.1 BANDWIDTH REQUIREMENT

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, we assume an overhead of 100% for our analysis. Let $B_b$ be the bandwidth required by an ITC to broadcast its messages. The value of $B_b$ can be expressed as:

$$B_b = \frac{N(42S + 4L_n + 10) + 69}{5000} \text{ Mbps}$$

(1)

Table 2 shows the bandwidth required by an ITC to broadcast its messages. From Table 2 it is seen that the maximum bandwidth required for broadcasting the messages is 0.349 Mbps.

<table>
<thead>
<tr>
<th>Number of Roads (N)</th>
<th>Number of Lanes per Road (L_n)</th>
<th>Number of Signal States per Road (S)</th>
<th>Length of message in Bytes</th>
<th>Bandwidth required in Mbps ($B_b$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>2</td>
<td>1</td>
<td>31.125</td>
<td>0.049</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>2</td>
<td>48.375</td>
<td>0.077</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>2</td>
<td>61.625</td>
<td>0.098</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>3</td>
<td>84.625</td>
<td>0.135</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>4</td>
<td>428.625</td>
<td>0.349</td>
</tr>
</tbody>
</table>

As explained in Section 3.2.1, the length of the message that has to be broadcasted by the vehicle is 96 bits. Let $N_v$ be the total number of vehicles at an intersection. Consider that the vehicles are communicating with the ITC every $t$ ms. Let $B_v$ be the bandwidth required by an ITC to accept messages from all the vehicles. If we consider an overhead of 100% in converting the raw bits into wireless packets, then the bandwidth $B_v$ can be expressed as:
Table 3 shows the bandwidth, $B_v$, required by an ITC to accept messages from $N_v$ vehicles. Table 4 shows the distance traveled by a vehicle in $t$ ms.

Table 3: Bandwidth, $B_v$, required by an ITC to accept messages from $N_v$ vehicles.

<table>
<thead>
<tr>
<th>Number of vehicles at intersection ($N_v$)</th>
<th>Bandwidth, $B_v$, 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>0.962</td>
</tr>
<tr>
<td>100</td>
<td>1.923</td>
</tr>
<tr>
<td>150</td>
<td>2.885</td>
</tr>
<tr>
<td>200</td>
<td>3.846</td>
</tr>
<tr>
<td>250</td>
<td>4.808</td>
</tr>
<tr>
<td>300</td>
<td>5.769</td>
</tr>
<tr>
<td>400</td>
<td>7.692</td>
</tr>
</tbody>
</table>

Table 4: Distance traveled by the vehicles in $t$ ms.

<table>
<thead>
<tr>
<th>Velocity of the vehicle (V) mph</th>
<th>Distance traveled by the vehicle in $t$ ms (feet)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>t=10 ms</td>
</tr>
<tr>
<td>30</td>
<td>0.44</td>
</tr>
<tr>
<td>40</td>
<td>0.58</td>
</tr>
<tr>
<td>50</td>
<td>0.73</td>
</tr>
<tr>
<td>60</td>
<td>0.88</td>
</tr>
<tr>
<td>70</td>
<td>1.02</td>
</tr>
</tbody>
</table>

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 ITC in feet. So there are maximum $\frac{R}{(L_v + 1.47V)}$ vehicles within the range of the ITC in each lane. The total number of vehicles at a given intersection with $N$ number of roads, $L_n$ lanes per road is

$$N_v = \frac{NL_n R}{L_v + 1.47V}$$ ................................................................. (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:

$$B_a = B_w - (B_b + B_v) \text{ Mbps}$$ ................................................................. (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 ITC is

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

Total time required for $N_v$ vehicles to authenticate the ITC is

$$T_{av} = N_v T \text{ µSec.}$$ ................................................................. (6)

From Equation 6, the maximum distance a vehicle can travel during the authentication process is given by
\[ D = \frac{1.47 T_p V}{10^6} \text{ ft} \] ................................................................. (7)

As explained in Section 3.2.2, the length of the digital certificate is 49 bytes. Table 5 shows the distance traveled by the vehicle during the authentication process for different ranges of ITC. Here the intersection is assumed to have four roads with four lanes per road. From Table 2, the bandwidth required for four roads with four lanes per road is 0.135 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 12 shows the time required for \( N_v \) vehicles to authenticate the ITC as a function of the vehicle speed for different communication ranges of the ITC. Figure 12 shows that for higher communication range of the ITC, more time is needed by the vehicles to authenticate the ITC. The reason is that as the range of an ITC increases, more vehicles are available with its range. Thus, more time is needed to authenticate the ITC by all the vehicles. Figure 12 also shows that when all vehicles are moving slowly, more time is needed for ITC 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 an ITC. Therefore, more time is needed to authenticate the ITC by all the vehicles within its range.
Table 5: Maximum distance traveled by a vehicle during authentication process (N=4, Ln=4, S=3)

<table>
<thead>
<tr>
<th>Range of ITC (R)</th>
<th>Velocity of the vehicle (V) mph</th>
<th>Number of vehicles at intersection (N_v)</th>
<th>Bandwidth required by N_v vehicles (B_v) mbps</th>
<th>Bandwidth available for authentication of N_v vehicles (B_a) mbps</th>
<th>Time required for authentication of N_v vehicles (T_{nv}) msec</th>
<th>Maximum distance traveled by a vehicle during authentication (D in ft)</th>
</tr>
</thead>
<tbody>
<tr>
<td>400</td>
<td>10</td>
<td>202</td>
<td>1.29</td>
<td>7.56</td>
<td>20.92</td>
<td>0.30</td>
</tr>
<tr>
<td>400</td>
<td>20</td>
<td>138</td>
<td>0.88</td>
<td>7.97</td>
<td>13.55</td>
<td>0.39</td>
</tr>
<tr>
<td>400</td>
<td>30</td>
<td>105</td>
<td>0.67</td>
<td>8.19</td>
<td>10.04</td>
<td>0.44</td>
</tr>
<tr>
<td>400</td>
<td>40</td>
<td>84</td>
<td>0.53</td>
<td>8.32</td>
<td>7.90</td>
<td>0.46</td>
</tr>
<tr>
<td>400</td>
<td>50</td>
<td>71</td>
<td>0.45</td>
<td>8.40</td>
<td>6.61</td>
<td>0.48</td>
</tr>
<tr>
<td>400</td>
<td>60</td>
<td>61</td>
<td>0.39</td>
<td>8.47</td>
<td>5.64</td>
<td>0.49</td>
</tr>
<tr>
<td>300</td>
<td>10</td>
<td>151</td>
<td>0.96</td>
<td>7.89</td>
<td>14.99</td>
<td>0.22</td>
</tr>
<tr>
<td>300</td>
<td>30</td>
<td>79</td>
<td>0.50</td>
<td>8.35</td>
<td>7.41</td>
<td>0.32</td>
</tr>
<tr>
<td>300</td>
<td>50</td>
<td>53</td>
<td>0.33</td>
<td>8.52</td>
<td>4.87</td>
<td>0.35</td>
</tr>
<tr>
<td>300</td>
<td>60</td>
<td>46</td>
<td>0.29</td>
<td>8.56</td>
<td>4.20</td>
<td>0.37</td>
</tr>
<tr>
<td>200</td>
<td>30</td>
<td>52</td>
<td>0.33</td>
<td>8.53</td>
<td>4.77</td>
<td>0.21</td>
</tr>
<tr>
<td>200</td>
<td>40</td>
<td>42</td>
<td>0.26</td>
<td>8.59</td>
<td>3.83</td>
<td>0.22</td>
</tr>
</tbody>
</table>

Figure 12: Time required for authenticating an ITC by all the vehicles within its range (for N=4 and L_n=4).
Figure 13 shows the distance that a vehicle will go through while it is authenticating an ITC. Figure 13 also shows that for an intersection with four roads and four lanes per road, the vehicles will move only a fraction of a foot during the ITC authentication process. Figure 14 shows similar results for an intersection with 8 roads and 8 lanes per road with an ITC range of up to 500 feet. Figure 14 shows that even for a very large intersection with 8 roads and 8 lanes per road in each direction, the vehicles will move only a few feet during the ITC authentication process. Thus, we can say that the time required for ITC authentication by all the vehicles is not too much, and it is acceptable for all practical purposes.

![Diagram showing distance traveled by vehicles during ITC authentication process for different ranges of the ITC](image)

**Figure 13:** The distance, a vehicle can travel during an ITC authentication process for different ranges of the ITC (for N=4 and L_n=4).
Figure 14: The distance, a vehicle can travel during an ITC authentication process for different ranges of the ITC (for $N=8$ and $L_n=8$)

4.2 MINIMUM REQUIRED RANGE OF AN ITC

A person needs about a second time to react to the warning and apply brakes to stop the vehicle. Let the speed of a vehicle at an intersection be $V_o$ feet per second (fps). Let us assume that an average driver can decelerate a vehicle at the rate of about $a$ feet/sec$^2$. From the basic laws of kinematics we have $S_v = V_o^2 / 2a$ feet, where $S_v$ is the distance traveled by the vehicle from the time the brake is pressed until the vehicle comes to the stop position. Tables 6 and 7 show the total distance traveled, with a reaction time of one second, by a vehicle before it stops after the warning has been issued.
Table 6: Distance traveled by a vehicle before it stops with a deceleration of 20 ft/sec\(^2\)

<table>
<thead>
<tr>
<th>Velocity (V) mph</th>
<th>Distance (S) feet</th>
<th>1 Second Reaction Distance (RD) feet</th>
<th>Total Distance (TD) feet</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>48</td>
<td>44</td>
<td>92</td>
</tr>
<tr>
<td>40</td>
<td>86</td>
<td>59</td>
<td>145</td>
</tr>
<tr>
<td>50</td>
<td>134</td>
<td>73</td>
<td>208</td>
</tr>
<tr>
<td>60</td>
<td>194</td>
<td>88</td>
<td>282</td>
</tr>
</tbody>
</table>

Table 7: Distance traveled by a vehicle before it stops with a deceleration of 15 ft/sec\(^2\)

<table>
<thead>
<tr>
<th>Velocity (V) mph</th>
<th>Distance (S) feet</th>
<th>1 Second Reaction Distance (RD) feet</th>
<th>Total Distance (TD) feet</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>65</td>
<td>44</td>
<td>109</td>
</tr>
<tr>
<td>40</td>
<td>115</td>
<td>59</td>
<td>173</td>
</tr>
<tr>
<td>50</td>
<td>179</td>
<td>73</td>
<td>253</td>
</tr>
<tr>
<td>60</td>
<td>258</td>
<td>88</td>
<td>346</td>
</tr>
</tbody>
</table>

Normally it takes some time for two wireless devices to establish a link after they come within their range. Let us assume that a vehicle needs one-second time to establish a wireless link with an ITC. On highways, the intersections are far away from each other and the speed limit is 55 mph. Let us consider a situation where a driver is going at 60 mph. Since an average vehicle can decelerate at the rate of 15 to 20 ft/sec\(^2\), from Table 7 we see that for a vehicle speed of 60 mph, the maximum distance traveled by a vehicle from the instance the warning is given until the vehicle is stopped is 346 feet. The distance traveled in one second during the link establishment time is 88 ft, and the distance traveled during the
ITC authentication process is under couple of feet at a vehicle speed of 60 mph (see Figures 13 and 14). Thus, the total distance traveled by a vehicle, from the time the vehicle starts communicating with an ITC until it stops when a warning is issued, is \(346+88+2 = 436\) feet. From the above analysis it is clear that on highways the range of an ITC should be greater than 436 feet.

In downtown areas, the intersections are closer to each other and the speed limit is 35 mph. Let us consider a situation where a driver is going at 40 mph. From Table 7, we see that for a vehicle speed of 40 mph, the distance traveled by a vehicle from the instance the warning is issued is 173 feet. The distance traveled during the link establishment time is 59 feet, and the distance traveled during the ITC authentication process is less than 2 feet. Thus, the total distance traveled by a vehicle, from the time the vehicle starts communicating with an ITC until it stops when a warning is issued, is \(173+59+2 = 234\) feet. Hence, for downtown areas the range of an ITC must be greater than 234 feet.

4.3 MEMORY REQUIREMENT

The memory required by the ITC to store the information of the vehicles approaching towards the intersection is in the order of some Kbytes. The ITC has to store the vehicles’ road number, velocity, acceleration and distance from the intersection. To store each vehicle’s information, the ITC needs four bytes of memory. Consider there are \(N_v\) vehicles at an intersection. The total memory required by the ITC can be expressed as

\[ M = 4 \times N_v \] Bytes.
Table 8: Memory required from an ITC

<table>
<thead>
<tr>
<th>Number of Vehicles ($N_v$)</th>
<th>Memory in Kbytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>0.023</td>
</tr>
<tr>
<td>24</td>
<td>0.093</td>
</tr>
<tr>
<td>48</td>
<td>0.187</td>
</tr>
<tr>
<td>75</td>
<td>0.292</td>
</tr>
<tr>
<td>100</td>
<td>0.390</td>
</tr>
<tr>
<td>150</td>
<td>0.585</td>
</tr>
<tr>
<td>200</td>
<td>0.781</td>
</tr>
<tr>
<td>300</td>
<td>1.171</td>
</tr>
<tr>
<td>500</td>
<td>1.953</td>
</tr>
</tbody>
</table>

From Table 8 it is seen that for 500 vehicles at an intersection, the maximum memory required by an ITC is 1.953 Kbytes. In addition to this memory, some memory is needed by ITC to keep the intersection information and for storing the digital certificates and run the program for maintaining the updated information. The size of this additional memory is fixed and doesn’t depend on the number of vehicles approaching towards the intersection.
Table 9: 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 roads at intersection</td>
</tr>
<tr>
<td>S</td>
<td>Number of signal states per road</td>
</tr>
<tr>
<td>Lₙ</td>
<td>Number of lanes per road</td>
</tr>
<tr>
<td>V</td>
<td>Velocity of the vehicle in Mph</td>
</tr>
<tr>
<td>R</td>
<td>Range of ITC in feet’s</td>
</tr>
<tr>
<td>Nᵥ</td>
<td>Number of vehicles at intersection</td>
</tr>
<tr>
<td>Lᵥ</td>
<td>Average length of the vehicle in feet’s</td>
</tr>
<tr>
<td>Bₜ</td>
<td>Total bandwidth available</td>
</tr>
<tr>
<td>Bₐ</td>
<td>Bandwidth available for authentication</td>
</tr>
<tr>
<td>Bₐᵇ</td>
<td>Bandwidth required for broadcasting messages</td>
</tr>
<tr>
<td>Bᵥ</td>
<td>Bandwidth required by Nᵥ vehicles</td>
</tr>
<tr>
<td>Lₜ</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>Tₐᵥ</td>
<td>Time required for authentication of Nᵥ vehicles</td>
</tr>
<tr>
<td>D</td>
<td>Distance traveled by the vehicle during the authentication</td>
</tr>
<tr>
<td>Sᵥ</td>
<td>Distance traveled by the vehicle during the application of brakes</td>
</tr>
<tr>
<td>Vₒ</td>
<td>Velocity of the vehicle in feet per second</td>
</tr>
<tr>
<td>a</td>
<td>Deceleration of the vehicle in feet/Sec²</td>
</tr>
</tbody>
</table>
5 CONCLUSION

This thesis work presented a secure wireless protocol for issuing intersection collision warnings. The thesis provided detailed description of the message format to be broadcasted and received by the ITC. A detailed description of the digital certificate format along with the authentication process between the ITC and the vehicles has also been presented. The thesis work also investigated the feasibility of implementing the Intersection Traffic Controller (ITC) and the protocol using the available technology. Suggestions are made to improve the functionality of the protocol for downtown areas where the intersections are very close to each other.
6  FUTURE WORK

When the intersections are very close to each other, say within 300 feet from each other, a vehicle that moves from the region of one ITC to another may not get enough time to establish a link with the new ITC, authenticate the new ITC and stop when a warning is issued unless the vehicle moves very slow, say under 30 mph. In this case, a vehicle may need to establish a link with the next ITC before it leaves the intersection of the previous ITC. In other words, the vehicle will communicate with two ITCs: the current one and the next one. However, before the vehicle leaves the intersection of one ITC, it will have limited communications with the ITC of the next intersection. We would like to investigate this case in our future work.
REFERENCES


[17] Syed Masud Mahmud, Shobhit Shanker and Srinivas Reddy Mosra


Transportation Research, Virginia Polytechnic Institute and State University, Blacksburg, Virginia)


[21] Website of Intelligent Transportation Systems Institute, Center for Transportation Studies, University of Minnesota.  
http://www.its.umn.edu/research/applications/ids/


[23] Website of Battelle Memorial Institute, Columbus, Ohio.  
http://www.battelle.org/news/96/11calspan.stm

[25] DSRC Tutorials, Website of DSRC.
   http://www.leearmstrong.com/dsrc/dsrchomeset.htm


ABSTRACT

DESIGN AND ANALYSIS OF A SECURE WIRELESS PROTOCOL FOR ISSUING INTERSECTION COLLISION WARNINGS

by

SRINIVAS R MOSRA

December 2004

Advisor: Dr. Syed Masud Mahmud

Major: Computer Engineering

Degree: Master of Science

According to NHTSA (National Highway Transportation Safety Administration), approximately 6.3 million crashes (50 percent of all crashes) occur at intersections every year causing over 9,612 fatalities and significant number of serious injuries. Radar and infrared technologies can be used to detect impending rear-end and lane-change collisions. However, impending intersection collisions cannot be detected using radar and infrared technologies, because these technologies require line-of-sight communications. Wireless communications do not require line-of-sight. Thus, Wireless communication technology will be a viable technology for detecting intersection collisions. In this thesis work, it is assumed that every vehicle is equipped with a wireless communication unit and every intersection has a wireless unit called the Intersection Traffic Controller (ITC). All vehicles near an intersection communicate with the corresponding ITC to send their dynamic information such as speed, acceleration, lane number, road number, and distance from the
intersection. Though the wireless technology will be a viable technology for developing intersection collision warning systems, it is subject to various types of security attacks unless the system is properly designed. This thesis work presents the detailed description of the architecture along with the secure wireless protocol for intersection collision warning systems with a detailed bit level description of the protocol. The security is maintained using a chain of digital certificates issued by various federal and state organizations. The vehicles validate the certificate of the ITC using the public key issued by a federal organization, such as the US Department of Transportation (USDOT). This thesis work also presents the performance analysis of the intersection collision warning system.
AUTOBIOGRAPHICAL STATEMENT

SRINIVAS R MOSRA

I received my Bachelors degree in Electrical and Electronics from J.N.T University, India. I have been working in the area of Intelligent Transportation System (ITS) for the past two and half years under the 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 intersection collision avoidance architectures.

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

Currently I am working as a software engineer with Borg Warner, Auburn Hills, Michigan. Apart from this stuff, I enjoy music, reading, bike riding, juggling, dancing, movies, sci-fi, and astronomy.

Publications:

