Detection and Report of Traffic Lights Violation Using Sensors and Smartphones

Francisco Martín-Fernández(✉), Pino Caballero-Gil, and Cándido Caballero-Gil

Departament of Computer Engineering, University of La Laguna, 38202 La Laguna, Spain
{fmartinf,pcaballe,ccabgil}@ull.edu.es

Abstract. Since technology is advancing at a rapid pace, new smart electronic devices are continually emerging to solve everyday problems. One of the most important problems of the world is related to road safety, so the mitigation of traffic accidents has become one of the biggest challenges for researchers. As a result, many proposals have emerged within the Intelligent Transport System (ITS) initiative. This paper proposes a new ITS-based system to automatically detect and warn about the breach of traffic lights. In the proposal, the vehicle that violates traffic lights self-reports of it, so the system can warn nearby vehicles to make they drive with greater caution. This self-reporting is done in a completely anonymously way so that users do not stop using the application. Besides, the method uses cryptographic algorithms to guarantee trust, integrity and authenticity of the information. The proposed system has been designed and implemented using sensors, smartphones and a server in the cloud, and the obtained results are promising.

Keywords: Road safety · Intelligent Transport System · Traffic light violation · Smartphone application

1 Introduction

Diverse problems related to road traffic have increased worldwide as a result of the population growth, ranging from big urbanized zones to dense populated areas. These traffic adverse circumstances can reduce the efficiency of transport infrastructure and increase travel time, fuel consumption and pollution. One of the consequences of the widespread of Information and Communication Technologies (ICT) is the existence of countless applications that help to drive.

Currently, decisions of drivers depend on what they see and/or hear. However, a system that includes interactive and cooperative driving and an effective traffic control would provide a third channel to receive additional data that cannot be directly seen or heard by drivers, but that might be very helpful for their decision-making.

The so-called Intelligent Transport System (ITS) is a set of technological solutions designed to optimize different modes of transport. One of its main

J.M. García-Chamizo et al. (Eds.): UCAmI 2015, LNCS 9454, pp. 237–248, 2015.
DOI: 10.1007/978-3-319-26401-1_23

purposes is to prevent adverse traffic circumstances, and to reach it, ITS is based on varied technologies.

Vehicular Ad-hoc NETworks (VANETs) are a key part of the ITS where information is exchanged among vehicles and/or with a communication infrastructure. Thus, every vehicle is assumed to have an information transmitter commonly known as On Board Unit (OBU). Regarding the communication infrastructure, it can be implemented in various ways. For instance, the infrastructure can be arranged along the road in the form of points of communication commonly referred as Road Side Units (RSUs).

A difficult problem in road safety is the discovery of users that fail to stop at red traffic lights. There may be several causes of traffic light violations. One of them is the duration of the traffic lights. Traffic lights with a very short duration cause that users ignore the red light, what produces a ripple effect that can cause many accidents. In order to try to overcome this problem, different solutions exist such as new traffic signal mechanisms, red-light speed cameras to detect offenders, etc., which reduce traffic jams in urban centers around the world. These solutions are effective but very expensive to be widespread.

According to the Traffic Safety Facts Report of the National Highway Traffic Safety Administration (NHTSA) [15], there were more than 2.3 million reported intersection-related crashes, resulting in more than 7,770 fatalities and approximately 733,000 injury crashes in the USA. In particular, the Fatality Analysis Reporting System (FARS) of the NHTSA reports that red-light running crashes alone caused 762 annual deaths, and that 165,000 people are injured annually by red-light runners. Besides, the Insurance Institute for Highway Safety (IIHS) reports that half of the people killed in red-light running crashes are not the signal violators, but drivers and pedestrians hit by red-light runners.

This paper is organized as follows. Section 2 briefly introduces some background of related work. Section 3 explains the theoretical solution proposed to protect the security of the scheme. Section 4 describes in detail the proposed scheme of the sensor platform. In Sect. 5, the user application of the system is presented. Section 6 provides a short explanation about the implementation of the proposal and its time performance. Finally, some conclusions and open problems close the paper in Sect. 7.

2 Related Works

The need of improving road traffic management is evident worldwide. Governments are worried about the growing number of vehicles on roads and of traffic-related deaths. For this reason, they are trying to improve traffic safety by exploring the potential of the ITS through numerous research projects funded by public entities and/or the automotive industry [1]. The current ITS state-of-the-art is based primarily on a series of initiatives from both academia and industry, addressed mainly to try to enable the future development of VANETs.

Several proposals exist to punish those users that violate traffic lights [4,5]. One of such proposals, called red light camera, has been operating for several years in regions such as China, Hong Kong, United Kingdom and North America [2]. A red light camera is a type of traffic enforcement camera that captures an image of any vehicle that enters an intersection after jumping a red traffic light. It takes automatically a picture to the vehicle that run the red light and the photo can be used as evidence that assists authorities in their enforcement of traffic laws. Generally, the camera is triggered when a vehicle enters the intersection (passes the stop-bar) after the traffic signal has turned red.

In [8], authors present an adaptive traffic light system based on wireless communication between vehicles and fixed controller nodes deployed in intersections. Such traffic light system is based on short-range wireless communication between vehicles, which uses a controller wireless node placed in the intersection that determines optimum values for the traffic lights phases.

The work from Google [7] presents several methods for automatically mapping the three-dimensional positions of traffic lights and robustly detecting traffic light state on board equipment in cars with cameras. They used these methods to map more than four thousand traffic lights, and to perform on board traffic light detection for thousands of drivers through intersections.

The work [11] proposes the use of RFID for dynamic traffic light sequences. It avoids problems that usually arise with systems that use image processing and beam interruption techniques. RFID technology with appropriate algorithm and database were applied to a multi-vehicle, multi-lane and multi-road junction area to provide an efficient time management scheme. A dynamic time schedule was worked out for the passage of each column. The simulation showed that the dynamic sequence algorithm could adjust itself even with the presence of some extreme cases. The conclusion is that the system could emulate the judgment of a traffic police officer on duty, by considering the number of vehicles in each column and the routing properties.

A modern traffic light for six roads and four junctions has been implemented by programming in the PIC16F877A microcontroller [12]. The system works efficiently over the present traffic controlling system with respect to less waiting time, efficient operation during emergency mode and suggestions of alternate route.

To the best of our knowledge, there is no proposal to notify the vehicles in an area where there is a nearby vehicle that has jumped a traffic light. Nor is there a solution allowing a vehicle to report that it has broken the law at a traffic light, anonymously. Anonymity can encourage using this system. The authorities can benefit by analyzing data generated by the system. In this way, it can detect if a traffic light is more likely to be violated than another one. Besides, this can serve to study and adjust the timing of traffic lights.

3 Security Scheme

The proposed system should maintain user anonymity, and integrity and authenticity of information, in order to promote the application to be used. The aim is not to find the users who skip the traffic lights, but to warn above that a user has jumped a traffic light, without being able to trace his/her identity. Therefore, a reliable and secure anonymity scheme is needed to inspire confidence to all users. The proposal uses a cloud server, a sensor platform and smartphones to achieve this aim. The smartphones are used to identify the vehicles. The sensor platform is located in traffic lights and communicates with the smartphones. The cloud server is responsible to notify to the other nearby vehicles.

In order to maintain this level of security, OpenSSL was used in the implementation. OpenSSL is an open-source implementation of the SSL and TLS protocols. OpenSSL supports a number of different cryptographic algorithms. In particular, this work uses the last version 1.0.2 released in January.

For the establishment of a secure communication channel, a Certificate Authority (CA) has been implemented in the cloud server. A certificate authority is an entity that issues digital certificates to certify the ownership of a public key. This allows others to rely upon signatures or on assertions made by the private key that corresponds to the certified public key. In this model of trust relationships, a CA is a trusted third party, trusted both by the subject (owner) of the certificate and by the party relying upon the certificate.

The integrity of the message and the authenticity of the sender are protected through the use of a digital signature scheme. Thus, the vehicle uses its private key during the process of digital signature of the message sent to the server, and the server uses the user's public key to verify the digital signature of the message. Specifically, the scheme is based on the Elliptic Curve Digital Signature Algorithm (ECDSA) [10] that offers a variant of the Digital Signature Algorithm (DSA), which uses elliptic curve cryptography.

The implementation is based on a digital signature scheme with the following parameters, where $\times$ denotes elliptic curve point multiplication by a scalar:

- $Curve$: Equation defining an elliptic curve field.
- G: Elliptic curve base point, generator of the $Curve$ with prime order n.
- n: Integer order of G, so that $n \times G = O$.
- d_A: Private key integer randomly selected in the interval $[1, n-1]$.
- Q_A: Public key curve point denoted by $Q_A = d_A \times G$.
- m: Message to sign.

On the one hand, n order to sign a message m, Algorithm 1 is used.

Algorithm 1. Signature Algorithm

1 Calculate $e = h(m)$, where $h(\cdots)$ is the SHA-3 cryptographic hash function;
2 Let z be the L_n leftmost bits of e, where L_n is the bit length of n;
3 Select a cryptographically secure random integer k from $[1, n-1]$;
4 Calculate the curve point $(x_1, y_1) = k \times G$;
5 Calculate $r = x_1 \bmod n$. If $r = 0$, go back to step 3;
6 Calculate $s = k^{-1}(z + rd_A) \bmod n$. If $s = 0$, go back to step 3;
7 The signature is the pair (r, s);

Algorithm 2. Verification Algorithm

Check that Q_A is not equal to the identity element O;
Check that Q_A lies on the curve;
Check that $n \times Q_A = O$;
Verify that r and s are integers in $[1, n-1]$. Otherwise, the signature is invalid;
Calculate $e = h(m)$, where $h(\cdots)$ is the same function used in the signature generation, SHA-3;
Let z be the L_n leftmost bits of e;
Calculate $w = s^{-1} \bmod n$;
Calculate $u_1 = zw \bmod n$ and $u_2 = rw \bmod n$;
Calculate the curve point $(x_1, y_1) = u_1 \times G + u_2 \times Q_A$;
The signature is valid if $r \equiv x_1 \pmod{n}$. Otherwise it is invalid;

On the other hand, each signature is verified by the server with Algorithm 2.

In order to protect user anonymity, k-anonymity is used for the digital signature. The concept of k-anonymity was first formulated in [14] as an attempt to solve the problem that given person-specific field-structured data, produce a data release with scientific guarantees that the individuals who are the subjects of the data cannot be re-identified while the data remain practically useful.

In particular, a release of data is said to have the k-anonymity property if the information for each person contained in the release cannot be distinguished from at least $k-1$ individuals whose information also appear in the release. In particular, the implemented schema guarantees k-anonymity through the application of the ideas in [3], according to vehicle every user is randomly associated to a group that share cryptographic material such as a par of privates pubic keys and a group certificate so that this data are used to sign. In this way, users do not reveal their particular identities but only their group identifier.

4 Sensor Platform

Sensing systems for ITS are based on networked system vehicles and infrastructures, i.e. on smart vehicle technologies. Infrastructure sensors are in general tough devices that are installed in the road. These sensors may be disseminated during road construction or by sensor injection machinery for rapid deployment. There are many types of sensors: vehicle counters, weather stations, cameras to detect traffic jams, radars to detect high speeds, etc. These sensors can be ranged from very simple (such as sensors to detect the number of vehicles on a road section) to highly advanced (such as cameras to detect vehicles with a special software). Usually, the more complex sensors are the most expensive. A camera with visual detection of vehicles is a very expensive system, and it is used to avoid the violations of traffic lights.

In order to add intelligence to traffic lights, the proposed system uses a light sensor that provides information in real time about the traffic light color. This, together with a Bluetooth Low Energy (BLE) module, allows transmitting the state of the traffic light to nearby vehicles, as a beacon notification.

Bluetooth road sensors are able to detect Bluetooth MAC addresses from Bluetooth devices in passing vehicles. If these sensors are interconnected, they are able to provide interesting data. Compared to other traffic measurement technologies, Bluetooth measurement has some differences:

- High Accuracy and the devices are quick to set up easily.
- Limited to a number of Bluetooth devices that can be broadcasting in a vehicle so counting and other applications are limited.
- Non-intrusive measurements what can lead to lower-cost installations for both permanent and temporary sites.

The sensor platform that is used consists of several electronic modules for composing a small, fully integrated system in any type of traffic light.

In this work, RFDuino [13], which is an Arduino shrunk to the size of a fingertip and made it wireless, is used as the board, exactly the 2216 model, with a Dual AAA Battery Shield. The shield has a step-up switching regulator that allows the batteries to be drained down to low voltages while still providing a stable 3.3 V to the RFduino.

The Bluetooth Low Energy module used for the RFDuino is the RFD22102 RFduino DIP. This module has the technical specifications shown in Table 1.

The format of a BLE message include a 1 byte preamble, 4 byte access codes correlated with the RF channel number used, a Packet Data Unit (PDU) that can be between 2 to 39 bytes and 3 bytes of CRC. Thus, the shortest packet would have 10 bytes and the longest packet would have 47 bytes. The transmission times of these packages range from 8 microseconds to the smallest package up to 300 milliseconds for the largest. The PDU for the advertising channel consists of the 16-bit PDU header, and depending on the type of advertising, the device address and up to 31 bytes of information. Also, the active scanner may request up to 31 bytes of additional information from the advertiser if the advertising mode allows such an operation. It means that a sizeable portion of data can be received from the advertising device even without establishing a connection. Advertising intervals can be set in a range of 20 ms to 10 s. It specifies the interval between consecutive advertising packets.

The sensor, which is connected to the traffic light, captures its color and state emitted by a beacon, and constantly sends this information to all vehicles near the traffic lights. To ensure the integrity of each beacon, a digital signature scheme is used.

ISO/IEC 9796-2 [9] scheme 1 based on SHA-1 hash and RSA is applied for the digital signature, because its length is only 22 bytes, so it fulfills the storage requirements of BLE beacons. ISO/IEC 9796-2 is a standard signature scheme widely used in the smart card industry for public key certificates and message authentication because it quite simple to implement.

All traffic lights have a generic certificate to sign beacons, given by the CA of the Directorate General of Traffic.

The beacon is formatted as shown in Fig. 1, where:

- idTrafficLight: Unique identifier for the traffic light.

Table 1. RFD22102 BLE Technical Specs

Specification	Value
Part number	RFD22102
Category	Bluetooth LE RF module
Type	Transceiver/Controller
Band	2.4 GHz
CPU	16 MHz ARM Cortex-M0
Flash	128 kb
Ram	8 kb
Multi frequency	Yes
Package-case	DIP RFduino footprint
Packaging	Bulk clamshell
RoHS compliant	Yes
Low supply voltage	1.9 V
Typical supply voltage	3 V
High supply voltage	3.6 V
Transmit current	18 mA, 4 uA ULP
Receive current	18 mA, 4 uA ULP
FCC approved	Yes
IC approved	Yes
ETSI CE tested	Yes
Transmit power	4 dbm

- bearing: Compass direction used to describe the direction of the traffic light (represented in degrees (0–360)).
- state: State of the traffic light (green, red, etc.)
- signature: Digital signature of the message.

This beacon is received by the smartphone, which is responsible for processing information and report anonymously if it did not respect the traffic signal.

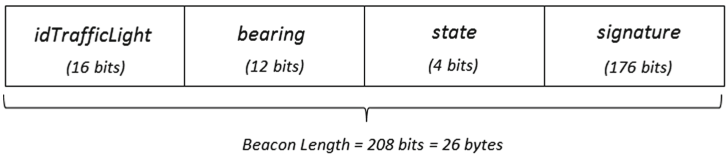

Fig. 1. Format of the beacon transmitted by the traffic light

5 User Application

A mobile application has been implemented to read the BLE beacon that the traffic light emits, and processes (See Fig. 2).

In order to monitor all system users and establish communications, including the use of a server, that is responsible for the control and monitoring, is proposed. The different system technologies are shown in Fig. 3.

Depending on the information contained in the beacon, and the speed that the vehicle has at that time, the application detects in background if the vehicle did not respect the traffic lights. If the vehicle driver violated the traffic light, the smartphone sends a message to a server that controls and manages such events. The server is responsible for searching its database to find nearby vehicles at

Fig. 2. User interface of the mobile application

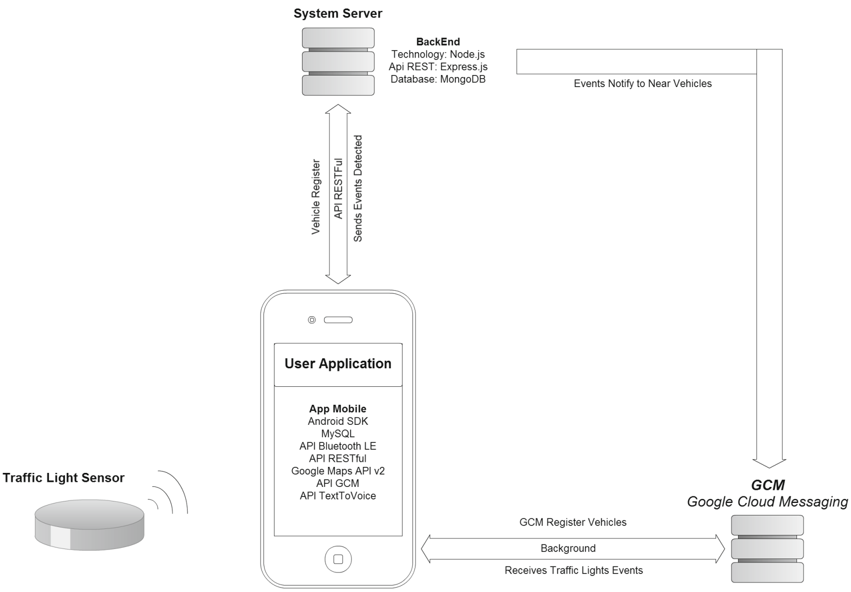

Fig. 3. Use flow and technologies used in the system

that time. This is possible because the server knows the position of each vehicle using the system, since all vehicles send every 5 seconds their current positions. Once it has located all vehicles near the traffic lights, a push notification that reaches all smartphones of nearby vehicles is generated. The application informs the driver via voice that there is another driver who has skipped a traffic light in its area, so it recommends driving with special caution. The application also displays on a map, the position of the traffic light.

The server is a full-stack Javascript implementation. As cross-platform runtime environment for server-side and networking applications Node.js is used. In order to connect the mobile application with the server through REST Web Services, the work uses Express.js. To store the vast amount of data on the server, a NoSQL database called MongoDB is used.

6 Implementation Analysis

The implemented system uses sensors, smartphones and cloud servers to automatically detect and anonymously report that a driver has failed to respect a traffic light. Figure 4 shows an overview of the system operation.

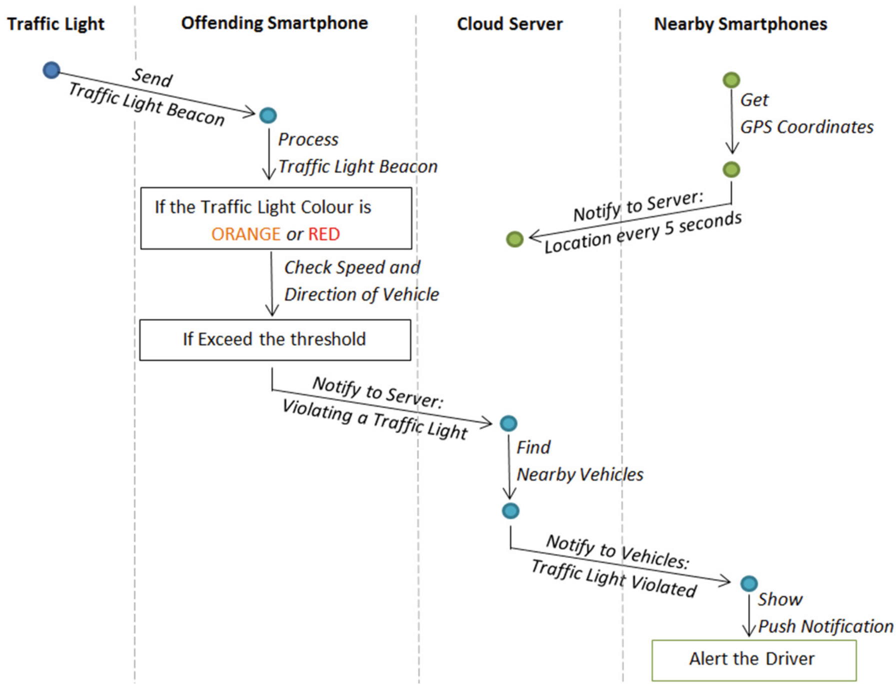

Fig. 4. Overview of the system operation

Table 2. Size of sent packets

Packet	Size (in bits)
Beacon from traffic light to smartphone (via BLE)	208
Data event from smartphone to server (via WiFi/GPRS/3G/LTE)	248
Push notification from cloud server to smartphones	272

The system can also be used by road authorities to detect traffic lights that are less respected. Thus, an action plan can be established to investigate the causes for searching solutions (longer duration of light color, etc.).

The system has several processes that send various data packets. In Table 2, the size of the different data packets used in the proposed system is shown.

Different batteries of tests were used to check the time separately for each scheme component and the total time. The simulations were done using multiple software packages to add credibility and develop a realistic simulation. Thus, the scenario that has been used for simulations comprises a real traffic situation in the city of Madrid (Spain) in 2014 [6] (See Fig. 5). In order to simulate the architecture and communications of a VANET, a tool called NS-2 was used, and for the traffic generation, we used SUMO software tool.

Fig. 5. Traffic simulation

Finally, the interaction between the traffic generated with SUMO and the network simulated with NS-2 was generated using MOVE, which allows users to rapidly generate realistic mobility models for VANET simulations.

As a result, the times represented by the averages of all tests, shown in Table 3, prove that efficiency has been achieved.

Table 3. Average time required to send different data

Component	Time (in Milliseconds)
Sending the beacon from the traffic light to the smartphone	0.17
Smartphone data processing	51
Sending event from smartphone to cloud server	116
Cloud Server data processing	104
Notification push from cloud server to smartphones	142
Total	**413.17**

7 Conclusions

Novel methods to try to avoid traffic accidents are becoming a major technological research. Among the main causes of traffic accidents, one of the most dangerous is the violation of traffic lights. There are several proposals to detect violators of traffic lights, but all are based on complex systems using video cameras to denounce such violators. This paper proposes a new system based on self-reports of offending vehicles in order to warn nearby vehicles. For this, the system makes use of sensors, placed at traffic lights, which emit their current status as beacon data. Each vehicle is paired with a smartphone that is responsible for reading and processing these beacons to discern whether the vehicle is violating traffic lights or not. If so, the smartphone notifies anonymously to a system in the cloud that the nearby traffic light has been violated. Then the cloud system notifies all nearby vehicles that there is a vehicle with outlaw behavior. The proposed system uses different cryptographic protocols to provide security to all communications and in particular to achieve anonymity, authenticity and integrity messages. This work is part of a work in progress but the first beta implementation shows promising results.

Acknowledgments. Research supported by TIN2011-25452, BES-2012-051817, IPT-2012-0585-370000, RTC-2014-1648-8 and TEC2014-54110-R.

References

1. Bin, T., Morris, B.T., Ming, T., Yuqiang, L., Chao, G., Dayong, S., Shaohu, T.: Hierarchical and networked vehicle surveillance in ITS: a survey. IEEE Trans. Intell. Transp. Syst. **16**(2), 557–580 (2015)
2. Bochner, B., Walden, T.: Effectiveness of red light cameras. Transp. Eng. J. **80**(5), 18 (2010)
3. Caballero-Gil C., Molina-Gil J., Hernandez-Serrano J., Leon O., Soriano M., On the revocation of malicious users in anonymous and non-traceable VANETs. In: XIII Reunion Española sobre Criptologia y Seguridad de la Informacion, pp. 87–91 (2014)

4. Charette, R., Nashashibi, F.: Traffic light recognition using image processing compared to learning processes. In: ICEE/RSI International Conference on Intelligent Robots and Systems, pp. 333–338 (2009)
5. Choi, C., Park, Y.: Enhanced traffic light detection method using geometry information. Int. J. Comput. Control, Quant. Inf. Eng. **8**(8), 1264–1268 (2014)
6. de Trafico, D.G.: Portal Estadistico Parque de Vehiculos. http://www.dgt.es/. Accessed 2015
7. Fairfield, N., Urmson, C.: Traffic light mapping and detection. In: IEEC International Conference on Robotics and Automation (ICRA), pp. 5421–5426 (2011)
8. Gradinescu, V., Gorgorin, C., Diaconescu, R., Cristea, V., Iftode, L.: Adaptive traffic lights using car-to-car communication. In: IEEE Vehicular Technology Conference, VTC2007-Spring, pp. 21–25 (2007)
9. ISO/IEC 9796–2:2010: Information technology, Security techniques, Digital signature schemes giving message recovery, Part 2: Integer factorization based mechanisms. ISO (2010)
10. Johnson, D., Menezes, A., Vanstone, A.: The elliptic curve digital signature algorithm (ECDSA). Int. J. Inf. Secur. **1**(1), 36–61 (2001)
11. Al-Khateeb, K.A., Johari, J.A., Al-Khateeb, W.F.: Dynamic traffic light sequence algorithm using RFID. J. Comput. Sci. **4**, 517–524 (2008)
12. Kham, N.H., Nwe, C.M.: Implementation of modern traffic light control system. Int. J. Sci. Res. Publ. **4**(6), 82–89 (2014)
13. RFDuino: http://www.rfduino.com/. Accessed May 2015
14. Sweeney, L.: k-anonymity: a model for protecting privacy. Int. J. Uncertainty Fuzziness Knowl. Based Syst. **10**(5), 557–570 (2002)
15. U.S. Department of Transportation, Traffic Safety Facts 2008 Report. National Statistics (2008)