Infrastructure to vehicle communications using inductive loops

Răzvan Andrei GHEORGHIU, Iulian BĂDESCU, Radu Şerban TIMNEA
Transport Faculty, Department of Telematics and Electronics in Transports
University POLITEHNICA of Bucharest
313, Splaiul Independenţei, Bucharest
ROMANIA
andrei.gheorghiu@upb.ro, iulian_badescu@yahoo.com, timrad66@yahoo.com; www.pub.ro

Abstract: Road safety is a worldwide issue. The constant increase of the number of vehicles and the more congested infrastructure lead to more traffic incidents. Infrastructure to vehicle communication is a way to improve traffic safety, by sending traffic information to vehicles, such as the colour the next traffic light will be when the car reaches the road junction. This approach may be useful also for autonomous vehicles that need all the data available in order to travel in a safe manner on the road network. In this article we shall analyse the possibility of sending information from the traffic management system to vehicles using one of the most common traffic detectors, the inductive loop.

Key-Words: communications, I2V, wireless, WiFi, Bluetooth, Zigbee, DSRC, urban traffic, traffic management system, inductive loop

1 Introduction

Information is very important in urban traffic management, both for vehicles and the system itself. The main data is obtained by traffic detectors, both in the pavement and on the road side and is used by traffic management algorithms to determine the best signalling times for the traffic recorded on the road network.

The drivers of vehicles, on the other side, get the information by direct observation of traffic conditions, which lead to relatively slow reactions to sudden changes and make the accurate prediction of the traffic ahead nearly impossible.

Is obvious that the drivers would benefit from the information the traffic management system has, but the communication between vehicles and infrastructure is complex and, usually, require special (expensive) equipment both in the vehicles and on the road side, without the immediate perspective of great benefits.

2 Problem Formulation

The information sent to the vehicles by traffic management system through road infrastructure would be very useful in taking the right decisions by drivers and helping avoid accidents.

In addition, autonomous vehicles are being studied in a lot of projects and are getting closer to the final stage – being able to travel in real traffic. These vehicles need all the information that may be obtained about the surrounding environment: other vehicles, the road infrastructure, junctions, signalling times and so on.

Vehicle-to-vehicle and vehicle-to-infrastructure communication systems are being studied in different implementations, but most of them implying additional equipment both in vehicles and in the road network system. This specialized infrastructure is usually not easy to implement, mainly due to the costs involved.

3 Existing systems

Infrastructure-to-vehicle (I2V) communications have been studied for some time, but mostly in air, naval and rail traffic. These solutions may represent a base for road communication systems.

We shall analyse in detail a safety rail system, considering the similarities to I2V for road traffic: similar speeds (lower for road traffic inside the cities), communication to only one vehicle at a time.

3.1 INDUSI System

"INDUSI" is an acronym derived from "**Indu**ktive **Si**gnalsicherung", or Inductive Signal Protection. The official term is PZB, for **P**unktförmige **Z**ug**b**eeinflussung, "spot-wise train control", as opposed to Linienzugbeeinflussung (LZB), linear train control.

According to some statistics [14], the INDUSI is the most popular train control system in Europe.

Table 1. Most popular train control systems in Europe [14]

System	Countries	Equipped track length
PZB/INDUSI	Austria, Germany, Romania, Serbia, Croatia, Slovenia	~75.000 km
Crocodile	France, Belgium, Luxemburg	~35.000 km
CCS-type systems	Czech Republic, Slovakia, Hungary, Italy, Netherlands	~19.000 km

This system was introduced in 1934, with the purpose of preventing running a red signal under almost any circumstance. Originally INDUSI provided warnings and enforced braking only if the warning was not acknowledged by the locomotive driver, but current developments provide more enforcement. [12]

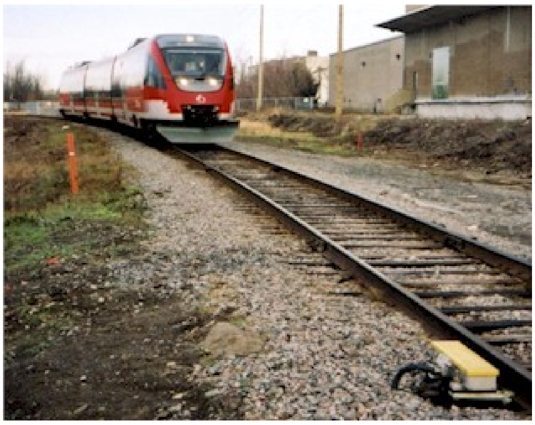

Fig. 1 INDUSI system [12]

The communication takes place by magnets that are mounted near the right rail. A similar magnet is mounted to the locomotive.

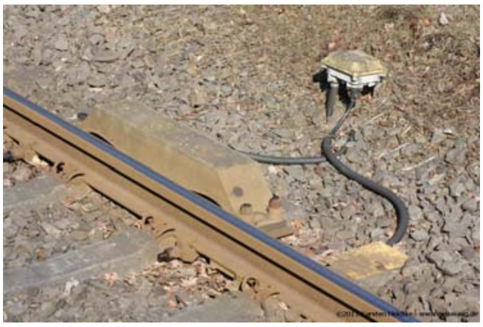

Fig. 2 INDUSI system – placement and cable connections [17]

The locomotive's magnet continuously emits magnetic fields with frequencies of 500, 1000 and 2000 Hz, respectively. These are sent to three resonance circuits, one for each frequency.

The trackside magnet contains a passive resonance circuit which is tuned to one of these frequencies and may either be switched on (active) or off (inactive). [12]

If the trackside switch is shorted there will be no current variation at the locomotive.

If the trackside magnet is active, it occur an increase of the locomotive resonance circuit’s impedance and, hence, a decrease of the voltage in the respective resonance circuit by 80-90%.

The action of the system depends on the frequency the trackside magnet is tuned to.

Then the locomotive passes over an active magnet tuned to 1000 Hz, the driver must acknowledge that he has understood the distant signal by pressing an attention button within 4 seconds, or the brakes will be applied.

After this, a speed check is performed, depending on the type of train.

The 500 Hz magnets are used to check the locomotive speed against some lower limits. This way, if the driver acknowledges the indication of the next signal but does not brake sufficiently or does not brake at all, the main signal is not passed at danger.

At the main signal there is a 2000 Hz magnet. This magnet will always cause an emergency braking when detected active by the locomotive. The train will come to a full stop before it reached the main signal. [12]

The track side equipment consists of:

- 1000 Hz magnets: are located at the distant signals, at permanent signals for sections with traffic dispatcher, at yellow marks for speed restrictions and yellow discs on portions with current line being closed.
- 500 Hz magnets: are placed in front of the signals, at a distance of 250 m from them. These magnets can be installed at a shorter distance, but not below 230 m.
- 2000 Hz magnets: are placed at the main signals.

The next figure illustrates the typical location of the magnets and the response required for the locomotive.

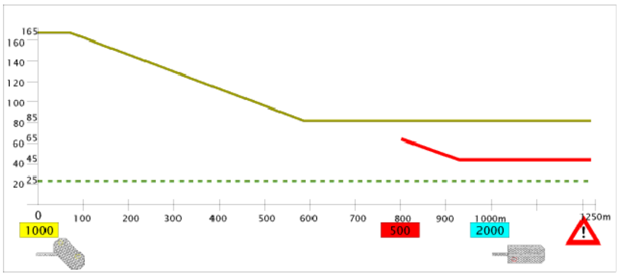

Fig. 3. Locomotive response for INDUSI magnets [12]

Schematic of the track installation is on the figure 4.

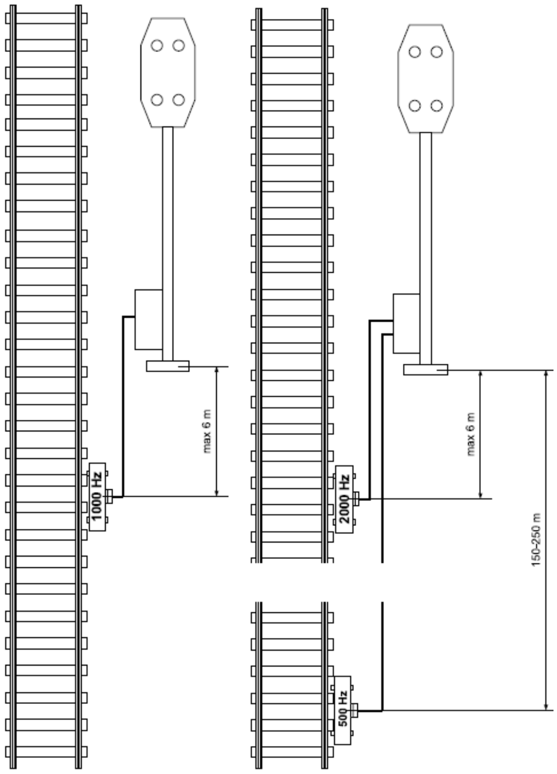

Fig. 4 INDUSI track side equipment installation [15]

The relation between the rail signal and the road side magnets is shown in the next table.

Table 2. Magnets' state depending on the rail signal

Signal	1000 Hz magnet	2000 Hz magnet	500 Hz magnet
Red	inactive	active	active
Yellow	active	inactive	inactive
Flashing yellow	active	inactive	inactive
Green	inactive	inactive	inactive

Before the trip, running mode for the train has to be selected. It can be selected internally, in the central AUTOSTOP unit, or externally. It is possible to select one of following running modes:

- E - ICE
- 1 - InterCity trains
- 2 - local and regional trains
- 3 - cargo trains

Each running mode has its own braking curve, which depends on train speed, maximum load and percentage of braking. Braking curves for running modes described above on figure 5.

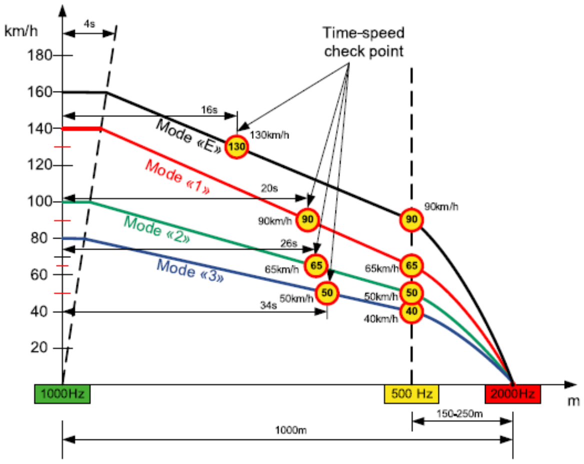

Fig. 5 INDUSI braking curves [15]

Some tests, both in laboratory and real life, have been performed [16] to estimate the data transfer average time for different data rates.

The performance tests have taken into account two key parameters: 'train-to-earth' data transfer average time; and average waiting time between each communication. The following tables shows the results obtained in two scenarios: without and with a Broadband Communications Manager [16].

Table 3. Results without the Broadband Communications Manager

Data Volume (MB)	Data Transfer Time (seconds)	Waiting time (seconds)
<1	1.10	0
1-10	11.30	0
11-50	58.84	0
51-100	184.62	0

Table 4. Results with the Broadband Communications Manager

Data Volume (MB)	Data Transfer Time (seconds)	Waiting time (seconds)
<1	0.76	0
1-10	7.69	0.76
11-50	38.46	8.45
51-100	115.38	49.91

4 Solution for road traffic

Inductive loops are already used by a lot of traffic management systems to detect number of vehicles passing over them. These are used for adaptive systems that can change the signalling times in junctions according to the real traffic recorded by the detectors.

Inductive loops are used in two ways: at the entry of the junction – to let the traffic controller know the number of vehicles approaching and at the exit of the junction – to transmit to the next traffic controller the number of vehicles that are going in that direction.

Considering this, inductive loops are used for the traffic management system to get the data needed for its algorithms.

But, as these are already installed in most of the traffic networks that have traffic management systems, we propose to use them not only to obtain traffic information, but also to send information from the system to vehicles. [2]

4.1 Inductive loops - basics

The inductive loop detector system is made of one (or more) wire loops embedded in the pavement (which represent the sensing component), a splice between the lead-in wire and the lead-in cable in the pull box, a lead-in cable connecting to the terminal strip in the controller cabinet, a cable from the terminal strip to the inductive-loop electronics unit, and the electronics unit. The connections between these components are shown in Figure 6. [3]

The magnetic flow is evenly generated along the loop, except the end portions. The intensity of the generated magnetic flow is [1]:

$$H = \frac{NI}{l} \qquad (1)$$

Where: H = magnetic flow intensity [A/m]
I = electric current [A]
N = coils number
l = resistor length [m].

Because the generated magnetic flow is even, the magnetic flow is:

$$\Phi = BA \qquad (2)$$

Where: ϕ = magnetic flow [Wb]
B = magnetic flow density [T]
A = loop section area [m^2]

The magnetic flow is dependent on the magnetic permeability:

$$B = \mu_0 \mu_r H \qquad (3)$$

Where: $\mu_0 = 4\,\pi 10^{-7}$ [H/m]
μ_r = relative permeability of the material (being 1 for air) [H/m]

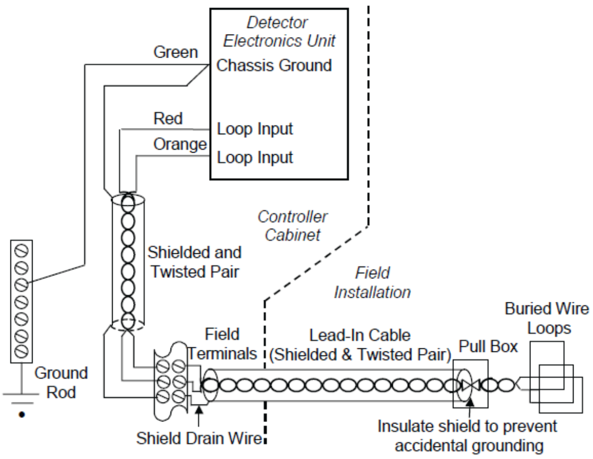

Fig. 6 Inductive-loop detector system [3]

Loop inductance is:

$$L = \frac{N\Phi}{I} = \frac{NBA}{I} = \frac{N\mu_0\mu_r HA}{I} = \frac{\mu_0\mu_r N^2 A}{l} \qquad (4)$$

When a vehicle is sensed by the loop, a small decrease in the loop inductance occurs, which is detected by the electronics unit.

The frequency range of typical electronics units is 20–60 kHz. Some units, that are able to provide vehicle classification, can operate at hundreds of kilohertz. Loop capacitance may cause the inductance sensed by the electronics unit to modify considerably with frequency if there are too many turns in the roadway loop. [3] This needs to be carefully planned in order to obtain the optimal sensibility of the detection system.

Some of the most important parameters that can be calculated based on inductive loops data are [4]:

a) Volume:

$$V = N/T, \qquad (5)$$

Where: V = detected vehicles/hour
N = detected vehicle in time interval
T = time interval [h]

b) Occupancy:

$$\theta = \frac{100}{T}\sum_{i=1}^{N}(t_i - D) \qquad (6)$$

Where: θ = occupancy [%]
T = time interval
t_i = total detector pulse time
D = descendent slope time – ascendant slope time

c) Speed:

$$v = \frac{3{,}6 \cdot 10^6 d}{5{,}280(t_1 - t_0)} \qquad (7)$$

Where: v = vehicle speed [km/h]

In case of using one detector:

d = vehicle length + detector length [m] (vehicle length is considered as an average)

t_0 = detection start time [ms]

t_1 = detection end time [ms]

In case of using two detectors:

d = the distance between the two detectors

t_0 = detection start time for 1st detector [ms]

t_1 = detection start time for 2nd detector [ms]

Based on the previous formula, the exact length of the vehicle can be deduced [4]:

$$L_v = \left(\frac{1}{2}\right)\left[(t_{11} - t_{10}) + (t_{21} - t_{20})\right]\left(\frac{5{,}280V}{3{,}6 \cdot 10^6}\right) \quad (8)$$

Where: v = previously established speed [km/h]

t_{i0} = detection start time for detector *i* [ms]

t_{i1} = detection end time for detector *i* [ms]

When the volume and the occupancy are known, speed is:

$$v = C\frac{V}{\theta} \quad (9)$$

Where: C = calibration coefficient, experimental determined.

4.2 Inductive loops occupancy time

The occupancy time of an inductive loop, in seconds, is:

$$t = \frac{L_v}{v} \times 3.6 \quad (10)$$

Where: t = occupancy time [s]

L_v = vehicle length [m]

v = vehicle speed [km/h].

The time a vehicle is above the inductive loop is important to be considered because this is the interval the communication between vehicle and infrastructure may occur.

There are 3 stages that can be identified:

1. The vehicle arrives above the detector; this causes the loop to react by decreasing its inductance. The electronic unit detects the modification and decide a vehicle was detected.
2. The electronic unit switch from reception (identification of changes in the loop circuit) to emission, in order to send information to the vehicle.
3. The actual communication infrastructure-to-vehicle takes place.

In order to evaluate the amount of data that can be sent, we first need to estimate the time available for the 4th stage. This is:

$$t_t = t - t_r - t_s \quad (11)$$

Where: t_t = transmit time

t = total time the vehicle is over the loop

t_r = total receive time

t_s = switch time from reception to emission

Considering a medium length of a car L_v = 4.3 m we may estimate the total time the vehicle is over the loop for different speeds inside the city:

- speed of 30 km/h:

$$t = \frac{4.3}{30} \times 3.6 = 0.516s \quad (12)$$

- speed of 40 km/h:

$$t = \frac{4.3}{40} \times 3.6 = 0.387s \quad (13)$$

- speed of 50 km/h:

$$t = \frac{4.3}{50} \times 3.6 = 0.3096s \quad (14)$$

- speed of 60 km/h:

$$t = \frac{4.3}{60} \times 3.6 = 0.258s \quad (15)$$

Thus, we may conclude that the time the vehicle is over the inductive loop is, most likely, between 0.258 and 0.516 seconds.

We shall consider an average loop response time of 100 ms, an approximate from two examples of loop datasheets ([5], [6]) one very fast and one slower, which have t_r of 10 ms and 150 ms.

We also have to consider a delay in the control unit when switching from receive to transmit mode. We estimate this delay, t_s, to be 50 ms.

With these values, in worst case (maximum speed – minimum time), from (11) we get:

$$t_t = 0.258 - 0.1 - 0.05 = 0.108s \quad (16)$$

Thus, the communication system will have to be able to transmit the information in 100 ms or less.

In the next section we shall present the basics of a communication system that may be implemented for data transmission to the vehicles using inductive loops.

4.3 Communication system

The concept of communication system based on inductive loops came from the INDUSI principle, used for railways: for the first stage of the system's implementation, there is only need to exchange little information, such as the colour of the traffic light when the vehicle will arrive at the next junction.

A two inductive loop system may determine the vehicle's speed and then, knowing its distance from the junction, the second loop may send to the driver the colour of the traffic light when the vehicle arrives at the junction, based on information obtained from the traffic management system.

The faster the communication system will be the more information may be exchanged between the vehicle and the traffic management system.

There are more solutions to implement the communication system. We shall focus on some protocols that are widespread used: Wi-Fi standard, Wi-Fi direct, Bluetooth, ZigBee and DSRC.

4.3.1 Wi-Fi protocol

Wi-Fi protocol is set in the IEEE 801.11 standards family. It was first defined in 1997 and further developed to allow faster communication between wireless equipment. Table 5 shows a brief history of IEEE 802.11.

Table 5. IEEE 802.11 standards family [7]

Standard	Description
IEEE 802.11	Up to 2 Mb/s; 2.4 GHz
IEEE 802.11a	Up to 54 Mb/s; 5 GHz
IEEE 802.11b	Up to 11 Mb/s; 2.4 GHz
IEEE 802.11g	Up to 54 Mb/s; 2.4 GHz
IEEE 802.11e	New coordination functions for QoS
IEEE 802.11f	Inter-AP Protocol
IEEE 802.11h	Use of the 5 GHz band in Europe
IEEE 802.11i	New encryption standards
IEEE 802.11n	MIMO physical layer

There are two operating modes for Wi-Fi standard: ad-hoc and infrastructure. The operating mode is selected during the configuration of the wireless station.

For the first mode, wireless stations communicate directly with one another, following a peer-to-peer model. Such networks can be set up anywhere, which is especially useful in situations requiring a quick setup.

The infrastructure operating mode requires one wireless access point (AP). A major role for an AP is to extend access to wired networks for the clients of a wireless network. All wireless devices trying to join must associate with the AP. [8]

At the beginning of a communication, the Wi-Fi equipment will scan the available channels to discover active networks. If a network is found, it will be selected. If the network is operating in infrastructure mode the device authenticates itself with the AP and then associates with it. If security is implemented, a further authentication step takes place, after which the station can participate in the network.

Wi-Fi is able to provide different degrees of quality of service, depending on the system required. It ranges from best effort to prioritise to the guarantee of services.

For our analysis, we select for data transfer the WiFi 802.11n protocol, which is supported by many devices and has the characteristics shown in the next table.

Table 6 WiFi 802.11n data rate

Frequency (GHz)	Bandwidth (MHz)	Data rate per stream (Mbit/s)
2.4/5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2
	40	15, 30, 45, 60, 90, 120, 135, 150

We may consider a bandwidth of 20 MHz and a rate of 28.9 Mbit/s, which should not be hard to obtain.

The amount of data that can be transmitted in 0.108 s is 3.1212 Mbit. There is a lot of data that may be included after the link is established. But the downside of Wi-Fi protocol is the four way handshake procedure that assures the accuracy of data being transferred. This requires time and reduces the amount of data that can be sent.

The messages exchanged during the handshake are depicted in Figure 7 and explained below.

To send a direct message to another node, the source node emits a Request To Send (RTS) packet, addressed to the intended destination. If that destination hears the transmission and is able to receive, it replies with a Clear to Send (CTS) packet.

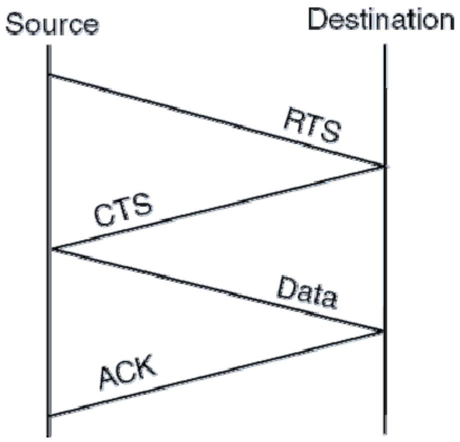

Fig. 7 Four way handshake [9]

The initiating node then sends the data, and the recipient acknowledges all transmitted packets by returning an ACK (Acknowledgement) packet for every transmitted packet received.

If specific data is sent, the transmission could be protected in order to ensure that the message only arrives to the intended receiver. WPS (Wi-Fi Protected Setup) was introduced and developed by the Wi-Fi Alliance to standardize and simplify ways of setting up and configuring security on wireless networks. [8]

4.3.2 Wi-Fi direct protocol

Wi-Fi Direct equipment can connect to each other without having to go through a typical access point, by embedding a software access point ("Soft AP"). This way, Wi-Fi Direct devices may establish their own ad-hoc networks.

Wi-Fi Direct is also referred to as Wi-Fi peer-to-peer or Wi-Fi P2P, as it functions in peer-to-peer mode.

When a device enters the range of the Wi-Fi Direct host, it can connect to it, and then gather setup information using a Protected Setup-style transfer. Connection and setup is very simplified and is intended to replace Bluetooth in some situations.

This protocol reduces the initial setup to a minimum and, hence, it is preferable to Wi-Fi standard for infrastructure-to-vehicle communication.

4.3.3 Bluetooth protocol

Bluetooth technology was defined in 1994, by Ericsson Mobile Communications. The goal was to obtain a low-power-consumption system for substituting the cables in the short-range area of its mobile phones and relevant accessories.

Bluetooth was adopted by IEEE 802.15 working group and made an IEEE standard, namely IEEE 802.15.1.

When a Bluetooth device is powered on, it tries to operate as a slave of an already running master device. It starts listening for a master's inquiry for new devices and responds to it with its address. This phase is not necessary for very simple paired devices that are granted to know each other's address.

Once a connection is established, the devices can optionally authenticate each other and then communicate. Devices not engaged in transmissions can enter one of several power- and bandwidth-saving modes or tear down the connection. Master and slave can switch roles.

Bluetooth security is divided into three modes:

- Non-secure
- Service Level enforced security (after channel establishment)
- Link Level enforced security (before channel establishment).

Authentication and encryption at the link level are handled by means of four basic entities:

1. the Bluetooth device address, a 48-bit unique identifier assigned to each device;
2. a private authentication key, which is a random number;
3. a private encryption key, also a random number;
4. a 128-bit frequently-changing random number, dynamically generated by each device.

There are two security levels for devices: trusted and untrusted, and three levels defined for services: open services, services requiring authentication and services requiring both authentication and authorization.

The protocol operates in the license-free band at 2.402–2.480 GHz. To avoid interfering with other protocols that use the 2.45 GHz band, the Bluetooth protocol divides the band into 79 channels (each one being 1 MHz wide) and changes channels, generally 1600 times per second. [10]

There are two forms of Bluetooth wireless technology systems: Basic Rate (BR) and Low Energy (LE). Both systems include device discovery, connection establishment and connection mechanisms.

The Basic Rate system offers synchronous and asynchronous connections with data rates of 721.2 kbps for Basic Rate, 2.1 Mbps for Enhanced Data Rate (EDR) and high speed operation up to 54 Mbps with the 802.11 AMP.

The LE system includes features designed to enable products that require lower current consumption, lower complexity and lower cost than BR/EDR. The LE system is also designed for use cases and applications with lower data rates and has lower duty cycles. [10]

Considering the maximum theoretical data rate of 2.1 Mbit/s, the amount of data that can be transmitted in 0.108 s is 232.2432 kbit. Bluetooth provides a quick connection method and, with some optimisations of the messages being sent, enough data rate to send the defined information to the vehicles.

4.3.4 ZigBee protocol

The first ZigBee specifications were set on December 14, 2004. After more revisions, ZigBee PRO was defined in 2007.

The ZigBee standard is built on IEEE 802.15.4 for packet-based wireless transport and enhances its functionality by providing flexible, extendable network topologies with integrated set-up and routing intelligence to facilitate easy installation and high resilience to failure.

ZigBee networks also incorporate listen-before-talk and rigorous security measures that enable them to co-exist with other wireless technologies (such as Bluetooth and Wi-Fi) in the same operating environment. The ZigBee standard operates in the 2400-MHz band, although it is possible to implement ZigBee networks in any other IEEE 802.15.4 bands. [11]

ZigBee is very flexible and allow networks to be easily adjusted to changing needs by adding, removing or moving network nodes. The protocol is designed such that nodes can appear in and disappear from the network, making it very adaptable and proper for infrastructure-to-vehicle communication. Another big advantage of a ZigBee network is the ease with which it can be installed and configured.

The configuration of the network depends on how the installed system has been developed. There are three system possibilities: pre-configured, self-configuring and custom.

a) Pre-configured system: all parameters are configured by the manufacturer. The system is used as delivered and cannot be modified or extended.
b) Self-configuring system: A system that is installed and configured by the end-user. The network is initially configured by sending "discovery" messages between devices. Some initial user intervention is required to set up the devices - for example, by pressing buttons on the nodes. Once installed, the system can be easily modified or extended without any re-configuration by the user - the system detects when a node has been added, removed or simply moved, and automatically adjusts the system settings.
c) Custom system: A system that is adapted for a specific application/location. It is designed and installed by a system integrator using custom network devices. [11]

The system is usually configured using a software tool.

ZigBee and IEEE 802.15.4 employ some techniques to ensure reliable communications between network nodes, such as Data Coding, Listen Before Send procedure and Acknowledgements.

All the reliability measures implemented allow a ZigBee network to operate even when there are other networks nearby using the same frequency band (ZigBee, Wi-Fi, Bluetooth, or other) without any interference.

The raw Zigbee data rate is 250 kbit/s per channel in the 2.4 GHz band. That means that the amount of data that can be transmitted in 0.108 s is 27 kbit.

This protocol has many advantages, mentioned above, but the data rate available may not be enough for some applications.

4.3.5 Dedicated Short Range Communication (DSRC) protocol

DSRC is the only wireless technology that can potentially meet the extremely short latency requirements for road safety messaging and control, but the current solutions are not fully field proven.

DSRC operates at 5.9 GHz frequency band with 75 MHz spectrum and a radius of approximately 1000 meters. In the 75 MHz spectrum, 5 MHz is reserved as the guard band and seven 10-MHz channels are defined as in shown in Fig. 8 (for US). The available spectrum contain one control channel (CCH) and 6 service channels (SCHs). The CCH is reserved, being used for carrying high-priority short messages or management data. All the other data are transmitted on the SCHs.[18]

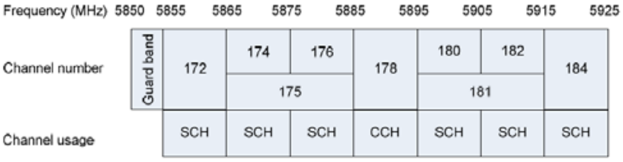
Frequency (MHz) 5850 5855 5865 5875 5885 5895 5905 5915 5925
Channel number
Guard band
172
174
176
175
178
180
182
181
184
Channel usage
SCH SCH SCH CCH SCH SCH SCH

Fig. 8. The DSRC frequency allocation in United States [18]

DSRC may provide a theoretical data rate of 6 to 27Mbps and is able to setup a communication between the infrastructure and vehicles that have speeds up to 160 km/h.

The main features of DSRC components are:

- For Road Side Unit:
    - announces to OBUs 10 times per second the applications it supports, on which channels
- for On Board Unit:
    - listens on channel 172
    - authenticates RSU digital signature
    - executes safety apps first, then switches channels
    - executes non-safety apps
    - returns to channel 172 and listens.

Due to the wide communication area and high-speed communication characteristics, DSRC is one of the most reliable road-to-vehicle communication methods available, and it can be used in many transportation applications, as presented in the figure below.

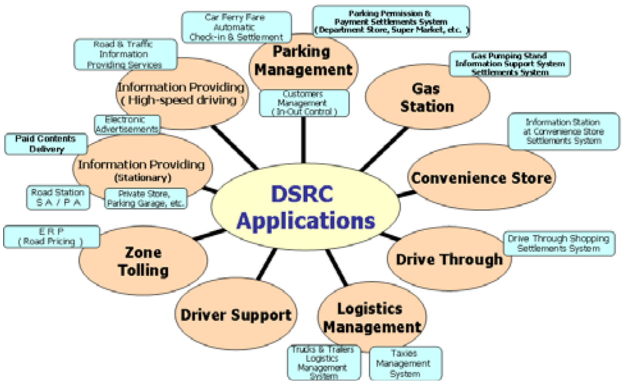
DSRC Applications
Parking Management
Car Ferry Fare Automatic Check-in & Settlement
Parking Permission & Payment Settlements System (Department Store, Super Market, etc.)
Customers Management (In-Out Control)
Gas Station
Gas Pumping Stand Information Support System Settlements System
Convenience Store
Information Station at Convenience Store Settlements System
Drive Through
Drive Through Shopping Settlements System
Logistics Management
Trucks & Trailers Logistics Management System
Taxies Management System
Driver Support
Zone Tolling
ERP (Road Pricing)
Information Providing (Stationary)
Paid Contents Delivery
Road Station SA / PA
Private Store, Parking Garage, etc.
Information Providing (High-speed driving)
Road & Traffic Information Providing Services
Electronic Advertisements

Fig. 9. DSRC Applications [19]

A specific example is the use of DSRC fo non-stop toll collection systems, especially for multi-lane applications, where vehicles can pass the toll gantry without reducing speed. Thus, DSRC enables the roadside equipment to interactively transmit and receive large volumes of data with multiple vehicles. One DSRC antenna can cover up to three free-flow lanes. The system also provides scalability toward other secured settlement via contactless IC card in OBUs and to other ITS applications.

The minimum DSRC data rate is 6 Mbit/s. That means that the amount of data that can be transmitted in 0.108 s is 664 kbit. Considering the maximum DSRC data rate of 27 Mbit/s, the amount of data that can be transmitted in 0.108 s is 2.9 Mbit.

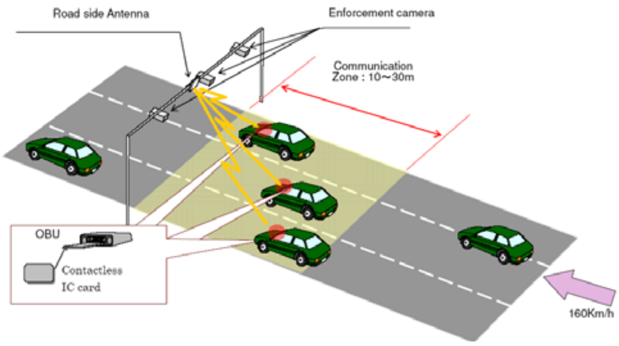

Fig. 10. DSRC Free-Flow Road Pricing System [19]

4.3.6 Comparison of the communication technologies presented above

In the next table we shall present a comparison between the technologies.

Table 7 Technology comparison

Technology	Advantages	Disadvantages
Wi-Fi	- Enough data rate for the necessary amount of data	- Four way handshake procedure
Bluetooth	- Quick connection method	- Optimisation needed, in order to increase the data rate
ZigBee	- Very flexible - No interference with other signals - Reliable communication	- Possible too low data rate
DSRC	- Very fast communication setup - Suitable for ITS applications	- Not fully proven in real life

Comparing the technologies from the data transfer point of view it result the next table.

Table 8 Technology comparison – part 2

Technology	Transmission time	Data rate
Wi-Fi	0.108 s	3.1212 Mbit
Bluetooth	0.108 s	232.2432 kbit
ZigBee	0.108 s	27 kbit
DSRC	0.108 s	664 kbit / 2.9Mbit

These results are comparable to the ones obtained in real tests for rail traffic. Considering the communication end-to-end delay and the call setup time, the protocols that seem to be more suitable for infrastructure-to-vehicle communications are Wi-Fi and DSRC.

5 Conclusion

Although some technical aspects that may alter the communication, such as noise and interference was not discussed in this article, the communication protocols presented offer enough capabilities and reliability to transmit information through loops.

In addition to already existing standards, a system developer could implement a proprietary wireless communication protocol that could optimize the access time and provide the optimum balance between security and data exchanged between vehicles and infrastructure. Such a procedure may benefit from the advantages the protocols described in this article have.

As all the calculus indicates, inductive loops may be used to transmit information to vehicles. Even though the vehicle speed is relatively high and there is little time available for the transmission, the modern communication techniques and devices allow the data exchange in these conditions.

Security issues should also be considered: wireless networks are, generally, less secured than the wired ones. [20] However, these aspects are well studied and there are solutions to improve the security of wireless communications. [21][22][23]

The next steps are to test such a system in laboratory and in real traffic conditions to determine the best communication method. The system may be further developed to allow bidirectional communication with the loops, in order for the vehicles to send useful information to the traffic management system, such as the direction it is going in the next junction, based on the in-vehicle GPS guidance system and other relevant data.

References:

[1] R.A. GHEORGHIU, I. BĂDESCU, R.Ș. TIMNEA, *Use of inductive loops to transmit information to vehicles*, ACMOS Conference 2014

[2] BUREȚEA L. D., CORMOȘ A. C., NEMȚANU F. C., MINEA M. TIMNEA R. Ș., IORDACHE V. GHEORGHIU R. A., System and method for assisting a vehicle driver in traffic, *RO-BOPI 10/2013*

[3] Lawrence A. Klein, Milton K. Mills, David R.P. Gibson, Traffic Detector Handbook, *Third Edition—Volume II, Publication No. FHWA-HRT-06-139*

[4] Gheorghiu RA, Urban traffic optimisations, *PhD Thesis, 2011*

[5] http://www.elektronika.ba/843/inductive-loop-vehicle-detector-v2-1/

[6] Clark Induction loop vehicle detector DB1 datasheet, http://www.clarksystems.co.uk/docs/datasheets/DB1_DATA_001.pdf

[7] Ferro Erina, Potortì F., Bluetooth and Wi-Fi wireless protocols: a survey and a comparison, *IEEE Wireless Communications magazine, 2004-06-30.*

[8] An Introduction to Wi-Fi, 019-0170 • 090409-B, *Printed in U.S.A., Digi International Inc. © 2007-2008*

[9] http://www.wildpackets.com/resources/compendium/wireless_lan/wlan_packets

[10] Bluetooth SIG, BLUETOOTH SPECIFICATION Version 4.1, 2013

[11] ZigBee PRO Stack User Guide, © NXP Laboratories UK 2012, JN-UG-3048, Revision 2.4

[12] http://www.sh1.org/eisenbahn/rindusi.htm

[13] Romanian Railway specifications

[14] EVOLUTION OF TRAIN CONTROL SYSTEMS, Béla Vincze, Géza Tarnai, *14th International Symposium EURNEX –ZEL 2006. Zilina, Szlovákia, 2006. pp. 69-76.*

[15] Automatic Train Protection System, ALTPRO product fiche

[16] Wireless Communications and Networks - Recent Advances, Wireless Technologies in the Railway: Train-to-Earth Wireless Communications, Itziar Salaberria, Roberto Carballedo and Asier Perallos, Deusto Institute of Technology (DeustoTech), University of Deusto, Spain, *Edited by dr. Ali Eksim, ISBN 978-953-51-0189-5, Publisher: InTech, March 14, 2012*

[17] http://www.geiswang.de

[18] An Overview of the DSRC/WAVE Technology, Yunxin (Jeff) Li, *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering Volume 74, 2012, pp 544-558*

[19] DSRC – NEW PRINCIPLES AND IMPLEMENTATIONS IN ITS ROMANIA, Florin Grafu, Angel Cormoș, Valentin Iordache, *Journal of Information Systems & Operations Management, 2009, vol. 3, issue 1, pages 157-166*

[20] A Secure Dominating set based routing and key management scheme in Mobile Ad hoc Network, R.PUSHPALAKSHMI, A.VINCENT ANTONY KUMAR, *WSEAS TRANSACTIONS on COMMUNICATIONS, Volume 10, 2011*

[21] Secure Communication Method Using Invitation Process in Mobile Ad Hoc Networks, Masao Tanabe, Masaki Aida, *WSEAS TRANSACTIONS on COMMUNICATIONS, Volume 11, 2012*

[22] Secured System against DDoS Attack in Mobile Adhoc Network, Arunmozhi Annamalai, Venkataramani Yegnanarayanan *WSEAS TRANSACTIONS on COMMUNICATIONS, Volume 11, 2012*

[23] Exploring Security Improvement of Wireless Networks with Directional Antennas, Hong-Ning Dai and Dong Li, Raymond Chi-Wing Wong, *36th Annual IEEE Conference on Local Computer Networks, Bonn, Germany, 2011*