Technology Survey of Wireless Communication for In-vehicle Applications

Md Ansarul Haque (MIT) & Md Delwar Hossain (EIS)

Master Thesis
30 ECTS

Halmstad, 2013
Technology Survey of Wireless Communication for In-vehicle Applications

Master Thesis

2013

Author: Md Ansarul Haque, MIT
mdahaq09@student.hh.se

Md Delwar Hossain, EIS
mddhos09@student.hh.se

Supervisor: Dr Kristina Kunert
Examiner: Professor Tony Larsson
Abstract

Currently, wireless communication technologies are expected to be widely employed for in-vehicle communication where in-vehicle communication is built upon the interactions of different parts inside the vehicle. This communication is to enable a variety of applications for driver and passenger needs. To have improved driving assistance, development of in-vehicle applications is very much needed. At present, intelligent systems inside the vehicle are mostly dominated by the wired technologies. The possibilities of wireless communication have inspired us and made an opportunity to analyse replacements for wired communication within a vehicle. In this connection, the scope of our thesis is to define the in-vehicle applications which are preferred by the wireless technologies, to define the applications using wired technologies which could be replaced by the wireless technologies and to identify those applications which are difficult to implement by the wireless technologies.

In-vehicle wired networks; and problems of these wired networks, along with several existing applications, have been discussed at the initial stage of this thesis for the purpose of having a clear understanding. After that, existing In-vehicle wireless applications and several challenging applications have also been studied. Studies have been done on the most important wireless technologies with their respective specifications. The requirement of establishing wireless communication has also been explained. Finally, an analysis has been done according to the requirements of the applications and verification of their possible reliance on the wireless technologies.

In a brief, comparable studies have been done among the wireless technologies to assess their current and future fitness for In-vehicle applications. The thesis concludes with some recommendations regarding when wireless technologies might be suitable for some in-vehicle applications to replace the wired technologies.

Index Terms:

Wireless Communication, TPMS, ETMS, WPAN, DSSS, FHSS, In-vehicle Applications.
Contents

Abstract ................................................................................................................................ iii

1 Introduction .................................................................................................................. 1
    1.1 Motivation ............................................................................................................... 1
    1.2 Problem Formulation and Research Questions ........................................... 1
    1.3 Methodology ............................................................................................................ 3
    1.4 Thesis Organization ............................................................................................... 3

2 Background and Application ................................................................................... 4
    2.1 Domain of In-vehicle Embedded Systems and Related Applications .......... 4
    2.2 Classification of In-vehicle Networks ................................................................. 6
    2.3 Traditional Wired In-vehicle Networks ............................................................... 7
        2.3.1 LIN ...................................................................................................................... 7
        2.3.2 CAN ..................................................................................................................... 7
        2.3.3 Byteflight ............................................................................................................ 7
        2.3.4 TTP/C ................................................................................................................... 7
        2.3.5 TTCAN ................................................................................................................. 8
        2.3.6 FlexRay .............................................................................................................. 8
        2.3.7 MOST ................................................................................................................ 8
    2.4 WSN Applications for In-vehicle Communication ............................................ 8
        2.4.1 Voice recognition and wireless internet connection .................................... 9
        2.4.2 Safety Assurance ............................................................................................... 9
        2.4.3 Security Assurance .......................................................................................... 9
        2.4.4 Maintenance and Diagnostics Services ......................................................... 9
        2.4.5 Tire Pressure Monitoring System (TPMS) ....................................................... 9
        2.4.6 Temperature Monitoring System ................................................................ 12
        2.4.7 Stall Removing System ................................................................................... 13

3 Wireless Technologies ............................................................................................ 14
    3.1 IEEE 802.15.1 ......................................................................................................... 14
        ➢ Protocols based on IEEE 802.15.1 .............................................................................. 16
        3.1.1 Bluetooth ........................................................................................................ 16
        3.1.2 WISA .............................................................................................................. 16
    3.2 IEEE 802.15.3/UWB ............................................................................................. 16
    3.3 IEEE 802.15.4 ......................................................................................................... 17
        ➢ Protocols based on IEEE 802.15.4 ......................................................................... 23
        3.3.1 ZigBee ............................................................................................................ 23
        3.3.2 6LoWPAN ..................................................................................................... 24
        3.3.3 Wireless HART .......................................................................................... 24
        3.3.4 ISA 100 ............................................................................................................ 24
        3.3.5 EnOcean ....................................................................................................... 24
        3.3.6 WiMi .............................................................................................................. 24
        3.3.7 SimpliciTi ...................................................................................................... 25
3.4 ANT .....................................................................................................................................25
3.5 WiFi ....................................................................................................................................25
3.6 Z-Wave ..............................................................................................................................25

4 Design Choice for Wireless Communication ......................................................................26

4.1 Operation Modes ...........................................................................................................26
4.2 Medium Access ...............................................................................................................27
4.3 Frequency, Data Rate and Range ..................................................................................27
4.4 Modulation and Signal Coding .....................................................................................28
4.5 Energy Consumption ......................................................................................................29
4.6 Security .............................................................................................................................32

5 Analysis ..........................................................................................................................37

6 Conclusion .......................................................................................................................42

Acknowledgments ..............................................................................................................43

References ..........................................................................................................................44
## List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AACN</td>
<td>Advanced Automatic Crash Notification</td>
</tr>
<tr>
<td>ABS</td>
<td>Antilock Braking System</td>
</tr>
<tr>
<td>ACL</td>
<td>Access Control List</td>
</tr>
<tr>
<td>AFH</td>
<td>Adaptive Frequency-Hopping Spread Spectrum</td>
</tr>
<tr>
<td>ASC</td>
<td>Automatic Stability Control</td>
</tr>
<tr>
<td>ASK</td>
<td>Amplitude-Shift Keying</td>
</tr>
<tr>
<td>ATC</td>
<td>Automatic Temperature Control</td>
</tr>
<tr>
<td>BO</td>
<td>Beacon Order</td>
</tr>
<tr>
<td>BPSK</td>
<td>Binary Phase-Shift Keying</td>
</tr>
<tr>
<td>CAN</td>
<td>Control Area Network</td>
</tr>
<tr>
<td>CAP</td>
<td>Contention Access Period</td>
</tr>
<tr>
<td>CCK</td>
<td>Complementary Code Keying</td>
</tr>
<tr>
<td>CFP</td>
<td>Contention Free Period</td>
</tr>
<tr>
<td>DPSK</td>
<td>Differential Phase-Shift Keying (DPSK)</td>
</tr>
<tr>
<td>DSSS</td>
<td>Direct Sequence Spread Spectrum</td>
</tr>
<tr>
<td>D/A</td>
<td>Digital-to-Analog</td>
</tr>
<tr>
<td>ECU</td>
<td>Electronic Control Unit</td>
</tr>
<tr>
<td>EPS</td>
<td>Electronic Power Steering</td>
</tr>
<tr>
<td>ETMS</td>
<td>Engine Temperature Monitoring System</td>
</tr>
<tr>
<td>FEC</td>
<td>Forward Error Correction</td>
</tr>
<tr>
<td>FFD</td>
<td>Full-Function Device</td>
</tr>
<tr>
<td>FHSS</td>
<td>Frequency Hopping Spread Spectrum</td>
</tr>
<tr>
<td>FSK</td>
<td>Frequency-Shift Keying</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>GFSK</td>
<td>Gaussian shaped, binary Frequency Shift Keying</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>GTS</td>
<td>Guaranteed Time Slots</td>
</tr>
<tr>
<td>Kbps</td>
<td>Kilo-bit-per-second</td>
</tr>
<tr>
<td>LIN</td>
<td>Local Interconnect Network</td>
</tr>
<tr>
<td>Mbps</td>
<td>Mega-bit-per-second</td>
</tr>
<tr>
<td>MIMO</td>
<td>Multiple-Input Multiple-Output</td>
</tr>
<tr>
<td>OFDM</td>
<td>Orthogonal Frequency Division Multiplexing</td>
</tr>
<tr>
<td>OQPSK</td>
<td>Offset Quadrature Phase-Shift Keying</td>
</tr>
<tr>
<td>PAN</td>
<td>Personal Area Network</td>
</tr>
<tr>
<td>PSK</td>
<td>Phase-Shift Keying</td>
</tr>
<tr>
<td>PSSS</td>
<td>Parallel-Sequence Spread Spectrum</td>
</tr>
<tr>
<td>QAM</td>
<td>Quadrature Amplitude Modulation</td>
</tr>
<tr>
<td>QPSK</td>
<td>Quadrature Phase-Shift Keying</td>
</tr>
<tr>
<td>RFD</td>
<td>Reduce-Function Device</td>
</tr>
<tr>
<td>RTS/CTS</td>
<td>Request to Send/Clear to Send</td>
</tr>
<tr>
<td>SAE</td>
<td>Society Automotive Engineers</td>
</tr>
<tr>
<td>SDP</td>
<td>Service Discovery Protocol</td>
</tr>
<tr>
<td>SIG</td>
<td>Special Interest Group</td>
</tr>
<tr>
<td>SO</td>
<td>Super-frame Order</td>
</tr>
<tr>
<td>SS</td>
<td>Spread Spectrum</td>
</tr>
<tr>
<td>STBC</td>
<td>Alamouti Space-Time Block Coding</td>
</tr>
<tr>
<td>TPMS</td>
<td>Tire Pressure Monitoring System</td>
</tr>
<tr>
<td>TTPA/A</td>
<td>Time -Triggered Light Weight Protocol</td>
</tr>
</tbody>
</table>
TPS  Throttle Position Sensor
UWB  Ultra-Wide-Band
WISA Wireless Interface for Sensors and Actuators
WSN  Wireless Sensor Network
Chapter 1

1 Introduction

1.1 Motivation

In-vehicle communication systems have been one of the most active areas of research in the field of automotive communication over the past and current decades. In this connection, vehicles and their different parts are increasingly connected to gather and distribute data, which could be used to enable better operations, performance, safety and comfort.

Gathering and distributing data by the use of typical wired sensor networks has always been expensive, with regard to installation and maintenance costs, also including the range limitation. These types of functional limitations of in-vehicle applications could be reduced by introducing wireless sensor networks i.e. wireless communication.

To resolve the problems of wired communication, wireless communication can be deployed. Wireless communication in a vehicle replaces wires that carry data between the vehicle’s controllers and the sensors with wireless links. This type of communication is a fast-growing technology to provide mobility and flexibility. It can potentially make a contribution in advanced communication and computation capabilities which refers to cost savings, mass (weight) savings and assembly simplification. It is usually used for monitoring purposes and work both in short- and long-range. It builds with a number of small sensing self-powered nodes which gather information or detect special events and communicate in a wireless fashion. These nodes help to sense, process and communicate which leads to a vast number of applications. To accommodate the new on-board sensors, wireless sensors (i.e., wireless networks) would also have major benefits. Wireless sensors would enable new sensor technologies to be integrated into vehicles as well as restrictive locations (such as tire pressure monitoring systems) to monitor the status of those locations.

This survey is also influenced by the applications of in-vehicle communication which could include: monitoring temperature inside/outside, tire pressure, fuel consumption, determining illumination failures (such as turn lights, front lights, back lights). [1] [2]

1.2 Problem Formulation and Research Questions

With the existing wired technologies, several difficulties are being faced by the implementers. Expensiveness of the wired systems, weight and difficulties to setup the wired systems in some sensitive and restricted areas are the major concerns. In vehicles, adding wire increases vehicle weight and therefore, weakens vehicular performance. An analysis of an average well-tuned vehicle reveals that every 50
kilograms of wiring – or extra 100 watts of power – increases fuel consumption by 0.2 litters for every 100 kilometres of travelling. [3]

The physical connections of the wires are usually shielded so they can be heat and interference resistant. As the number of sensors increases, the shielded copper wires also increase which means more expenses. To design the layout of those wires in the vehicle requires technical and engineering effort which is also introducing costs. Wires and wiring harnesses do have more weight, as well as more and longer wires being needed which eventually increases the heaviness [4]. Therefore, the physical wiring in the vehicle might have an impact on the overall performance.

In the vehicle, some locations are restricted where current wired communication cannot be deployed. Such locations are steering wheels or tires. For example, tire pressure monitoring systems in the vehicle would be impossible for the wired system integration. [4] Reengineering of sensors and communication infrastructure are needed in every production cycle. Additionally, it requires significant efforts to accommodate the growing demand for on-board sensors without adding physical capacity or change the location of a sensor, compared to the existing design.

As we also know, more networks pursue more cost. Therefore, we need a single network which is able to handle all needs of the vehicle rather than already having dedicated buses for different applications. [5] In this aspect, a big problem on the vehicle is mass (up to 50 kg) and cost of implementation. A modern vehicle has more than hundreds of connection points which are composed of several km of wires or cables. It raises big issues of complexity for maintenance and diagnostic checks. [6] With reference to all these problems, the research community provided a possible solution, based on wireless communication technology. This type of technology gives us a very good prospective in aspect of size, cost; and weight. It also gives the opportunity to sense an element or take information where the wire is unreachable.

It is also to be noted that wireless communication is always threatened by having limited resources alongside the security and reliability issues. Wireless communication faces the challenge of propagation loss, shadowing and multi-path fading. Propagation loss depends on the distance from the source to destination and multi-path fading is due to the fact of the presence of multiple paths between the source and destination. The challenges of achieving energy and bandwidth efficiency, plus the higher data rate of different applications are also of concern for wireless communication. [7]

So, the research questions of this thesis stand as:

• Which in-vehicle applications can rely on and benefit from using wireless communication?
• Which wired applications could be replaced by the wireless communication?
• Which applications would face difficulty in case of using wireless communication?
1.3 Methodology

This thesis considers wireless communication for in-vehicle applications with proper reasoning. In-vehicle applications could favor wireless communication because of their advantages over the wired communication. Therefore, if we can erase the limitations of the wired communication by the wireless communication, it would have very much possibility to replace them for in-vehicle applications. Usually wireless communication is less expensive than wired communication. Now it is much needed to analyze that whether the requirements of wireless communication are proportionally equal or more effective against the requirements of the wired communication for those applications. Later the requirements or demands of in-vehicle applications will be considered accordingly against the characteristics of wireless technologies.

Initially we will go through the domain and classes of in-vehicle systems and networks. Existing wired networks or technologies are followed by the existing wireless technologies. Literary work and comparative study of these technologies will be discussed with their characteristics and requirements. We shall conclude with the remark about which in-vehicle applications are suitable for wireless technologies, which applications could replace the wired technologies by the wireless technologies as well as the applications which are presently facing difficulty in case of wireless communication.

1.4 Thesis Organization

This thesis conducts a survey on wireless communication where in-vehicle applications and their needs are the concerning factors. The Introduction in Chapter one is followed by the background and applications of in-vehicle applications in Chapter two. Chapter two includes the domain of in-vehicle systems and classification of networks, traditional wired networks and their wireless in-vehicle applications. A brief explanation of different wireless technologies is illustrated in Chapter three. Preferred requirements for establishing wireless communication are also described in Chapter four to assist technical analysis. Finally, an analysis has been done in the field of wireless communication focusing on in-vehicle applications in Chapter five followed by conclusion of the thesis paper in Chapter six.
Chapter 2

2 Background and Application

Vehicles of the modern age are being deployed with an ever increasing number of sensors for the sake of safety, comfort or convenience and performance. As a result, an increasing number of electronic control units (ECU) as well as communication signals with more complex interrelations are introduced to meet the requirements. Such developments in automotive electronics reveal the need for dependable, efficient, high-speed and low cost in-vehicle communication. This study presents the summary of a technical survey on in-vehicle communication network including different in-vehicle system domains and their respective applications those have been used in automobiles or are likely to be used in the near future.

2.1 Domain of In-vehicle Embedded Systems and Related Applications

In-vehicle embedded systems can be classified into five functional domains based on the architecture, properties and constraints [1]. The functional domains of an in-vehicle embedded system are named as chassis domain, powertrain domain, body domain, telematics domain and passive safety domain.

i. Chassis Domain:

   Chassis domain has the functionality of advanced real-time control systems, which is having safety critical applications with strict timing requirements. It is usually used for driving dynamics and assistance. X-by-wire applications are included in the domain where ‘x’ is represented for brake, steer or throttle. Though in general terms, X-by-wire is for replacement of mechanical and hydraulic automotive systems with electronic systems. Chassis domain with the safety critical applications requires high bandwidth and flexibility and; high dependability to some extent. In this domain, dependability and bandwidth requirements make solutions of time-triggered and hybrid approaches for in-vehicle networks.

   Applications:
   - ABS (Antilock Braking System)
   - ASC (Automatic Stability Control)
   - EPS (Electronic Power Steering)

ii. Powertrain Domain:

   The Powertrain domain has the functionality of complex control mechanisms including high computing complexity. It is usually used for generating power in the engine and, transmitting of power through the gear box to the driving axis and wheels. Frequent data exchanges between chassis and body domain are also maintained by this domain with strict timing requirements.
Therefore, high bandwidth, high dependability and predictability in communication are required for this domain. If the network condition of this domain is stable and well-defined, a low degree of flexibility would be enough.

**Applications:**
- Engine control
- Transmission control
- Gear control

### iii. Body Domain:

Body domain has the functionality to implement body or comfort functions. The applications of body domain are not required of high bandwidth as well as not required of safety criticality. Low cost networks are implemented in this domain for this type of communication.

**Applications:**
- Air conditioning and climate control
- Lights, seats, mirrors, locks, wipers, doors, windows, park distance control

### iv. Telematics Domain:

Telematics domain has the functionality related to multimedia, infotainment and wireless sub-domains. A huge amount of data is exchanged in this domain. QoS; and security are more important for the networks in this domain. Most importantly, the communication of this domain partially depends on the outside communication where information are gathered from external environment and used for internal purpose. This study has taken only the in-vehicle communication excluding the outer communication.

**Applications:**
- GPS and in-vehicle navigation systems
- Rear seat entertainment
- Audio Systems and CD/DVD players
- Monitors and displays
- Voice Recognition and wireless internet connections

### v. Active Safety Domain:

Chassis domain control approach is very much closer to active safety domain approach. To retain maximum control of the vehicle, the applications of active safety domain are needed to consider. This active safety domain monitor’s on-road dynamics to proactively prevent vehicles from colliding with each other or with other objects as well as it helps to ensure the control of the vehicle when normal tolerances are exceeded. [36]
Applications:
- ESC (Electronic Stability Control)
- ABS (Anti-lock Braking System)
- EBS (Electronic Brake Assist)

vi. Passive Safety Domain

A Passive safety domain serves the safety related functions. Therefore, it requires high dependability; and predictability as well as high speed data transmission. This domain employs systems such as impact, rollover sensors; and airbags.

2.2 Classification of In-vehicle Networks

According to the Society Automotive Engineers (SAE), in-vehicle networks are classified into the following classes/categories [1] [5] [6]:

Class A: This type of network is used for low-end, non-emission diagnostics and general purpose communication. It must support event-driven message transmission and bit rate is less than 10 Kbps. Class A networks such as Local Interconnect Network (LIN) and Time -Triggered Light Weight Protocol(TTPA/A) are used mainly as simple control data related applications to the body domain such as seat control, rain sensor, doors etc.

Class B: This type of network is used for the vast majority of non-diagnostic, non-critical communication (such as instrument cluster, vehicle speed, legislated emissions data, etc) those are J1850 and low speed Controller Area Network (CAN-B). It must support event-driven and some periodic message transmission, plus sleep/wakeup and the data rate is between 10 Kbps and 125 Kbps.

Class C: This type of network is used for faster, higher bandwidth systems such as engine timing, fuel delivery, etc. It must support real-time periodic parameter transmission and the data rate is between 125 Kbps and 1 Mbps (used in the powertrain and the chassis domain). The examples of this type network is High speed CAN-C.

Class D: This type of network is used for much faster, higher bandwidth systems, high speed communication (the data rate is 1 Mbps or above) and are used for telematics (multimedia, infotainment, internet, digital TV, etc) and x-by-wire application. FlexRay and Time Triggered protocol (TTP/C) are used in this class.

The following Table-2.1 gives an explanation of Class A, B, C and D regarding to their respective domain, speed, data rate and in-vehicle applications. Class A and B mostly perform the Body domain applications. Class C and D do perform the in-vehicle applications of powertrain and chassis domain, telematics domain respectively.
<table>
<thead>
<tr>
<th>Network</th>
<th>Class A</th>
<th>Class B</th>
<th>Class C</th>
<th>Class D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Body (Mostly dedicated)</td>
<td>Body</td>
<td>Powertrain and chassis</td>
<td>Telematics</td>
</tr>
<tr>
<td>Speed</td>
<td>Low</td>
<td>Higher</td>
<td>Higher</td>
<td>Higher</td>
</tr>
<tr>
<td>Data rate</td>
<td>&lt; 10 kb/s</td>
<td>10 kb/s to 125 kb/s</td>
<td>125 kb/s to 1 Mb/s</td>
<td>&gt;= 1 Mb/s</td>
</tr>
<tr>
<td>Examples</td>
<td>Low cost applications</td>
<td>General information exchange (i.e. vehicle speed)</td>
<td>Especially for wide range of applications</td>
<td>Multimedia and infotainment data</td>
</tr>
</tbody>
</table>

Table 2.1 In-vehicle networks according to their respective requirements [1]

2.3 Traditional Wired In-vehicle Networks

The main traditional wired in-vehicle communication networks are explained as follows [1]:

2.3.1 LIN

Local Interconnect Network (LIN) is a low speed (20 Kbps) and low cost serial bus in-vehicle communication network. LIN is widely used in the body domain of the vehicle because of its simple and low-cost feature. It is also used for some comfort functions.

2.3.2 CAN

Controller Area Network (CAN) is a serial bus developed by Robert Bosch GmbH. At present, CAN is the de-facto standard for in-vehicle data transmission with data rates ranging from 125 kbps to 1 Mbps and mostly used for automotive communication for its flexibility and robust communication, including its bounded delay, simplicity and low-cost.

2.3.3 Byteflight

Byteflight is developed by BMW and it has the data rate of 10 Mbps. Byteflight requires high bandwidth and it is used for highly safety related (i.e. passive safety) networks for automobiles.

2.3.4 TTP/C

Time-Triggered Protocol (TTP/C) offers the data rate up to 25 Mbps and it is based on the TDMA mechanism. It is complex in design and also leads to higher costs. A TTP frame contains 240B of data and 4B of overhead. A communication schedule
makes the TTP/C protocol less flexible but its time-triggered manner allows itself to be predictable and composable.

2.3.5 TTCAN

Time-Triggered Controller Area Network (TTCAN) is also developed by Robert Bosch GmbH and it is based on the TDMA mechanism. TTCAN uses the same standards and message formats as CAN (data rate is 125 kbps to 1 Mbps) but in contrast to CAN, it has a master node to provide time synchronization among nodes.

2.3.6 FlexRay

FlexRay is used for high-speed and flexible in-vehicle communication and it offers bit rate up to 10 Mbps. It seems to be the best choice for the safety-related applications and future high-speed automotive applications.

FlexRay is based on the TDMA and FTDMA mechanisms. It offers star and multiple star network topologies. The network exchanges messages which contain 254 B of data with 5 B of header.

2.3.7 MOST

Media Oriented Systems Transport (MOST) is developed to facilitate in-vehicle multimedia and infotainment systems with a data rate of up to 24.8 Mbps during the transmission of audio, video, data and control information. It offers a data-efficient and cost-effective communication infrastructure.

2.4 WSN Applications for In-vehicle Communication

Wireless Sensor Network applications for in-vehicle communication constitutes a challenge for researchers and a large amount of research projects in this area are working on identifying them. WSNs should be capable to collect, process, and supply the user with several types of technical information about the vehicle. This chapter sheds light on some of the examples of existing in-vehicle applications as well as an explanation of WSN applications such as identification of wrong tire pressure value, monitoring temperatures; and assisting brakes.

A number of new services and applications are able to be introduced into a vehicle by integrating wireless communication technology. By using this technology, the vehicle acquires new capabilities and offers more services to its users.

Several units of the vehicle enable the deployment of these following features [8]:

8
2.4.1 Voice recognition and wireless internet connection

The users of the vehicle can send and receive a voice activated email while on the road.

2.4.2 Safety Assurance

Information gathering from the vehicle’s surroundings is useful for these safety systems i.e. the communication between the vehicle and its surroundings, e.g., roadside objects and other vehicles. The provided facilities of these systems are unsafe driving profiling, collision avoidance systems, accident and roadside assistance; and intelligent airbag deployment systems.

The Advanced Automatic Crash Notification (AACN) system of General Motors (OnStar™-equipped vehicles) is an example of this type of safety system.

2.4.3 Security Assurance

Tracking services of stolen vehicles and vehicle antitheft are featuring securities for a vehicle. OnStar™-equipped vehicles provide the remote door unlocking services.

2.4.4 Maintenance and Diagnostics Services

Some services could be done remotely, such as maintenance systems as well as diagnostics, vehicle and driver monitoring.

2.4.5 Tire Pressure Monitoring System (TPMS)

A tire pressure monitoring system (TPMS) is an electronic system designed with WSNs to monitor the air pressure inside the pneumatic tires on various types of vehicles. Smart tires, i.e., intelligent tires, are equipped with sensors for monitoring quantities such as air pressure, temperature, wheel loading, friction; and are expected to improve the reliability of tires and tire control systems. This system reports real-time tire pressure information to the driver of the vehicle by a pictogram display or a simple pressure warning alert, when the pressure is low or dangerous. This system employs pressure or other sensor types, plus a reliable method for transferring data from inside a pneumatic tire to alert drivers when tires are under-inflated.

Recent studies report that adverse road conditions and tire defects play a major role in road traffic accidents. In this regard, it is a matter of urgency from a traffic safety point-of-view, to introduce intelligent tires with a warning system for road conditions, optimizing control on poor surfaces; and a tire defect detection system that measures tire deformation, in addition to a TPMS. [9]

TPMS uses two important key technologies for the intelligent tires. Those are:

- Wireless sensors and
- Data transmission methods.
For installing sensors to measure strain applied to a tire, we have to consider different factors:

- The stiffness of the tire rubber is very low. The high stiffness difference may cause de-bonding of sensors from the tire rubber or degrading performance of the tire because wireless sensors themselves inhibit the deformation of the tire.
- It is spatially impossible that large-sized sensors are installed in a special environment such as the interior space of the tire. Moreover, it is economically difficult to use expensive sensors, because tires are comparatively inexpensive products.

In terms of the data transmission, we have to consider different factors:

- When sensors are installed inside the tire, wireless monitoring is indispensable.
- Moreover, to activate the sensor, it is necessary to install a battery in the tire. The battery, however, has a limited life and it is difficult for tire users to replace the battery inside the tire.

For the second requirement, energy harvesting or energy scavenging that converts mechanical vibration of tires to electric power could be a good choice to eliminate the need for battery replacement. The sensor also has the advantages of decreasing fuel consumption and off-balance problems of the tire, due to sensor installation.

In [10], this review therefore discusses two key technologies of intelligent tires:

1) Tire sensing technology that involves a TPMS and is used in developing an advanced intelligent tire with a tire deformation, wheel loading, or friction measurement system, and

2) A system for wireless data transmission between tires and the vehicle that involves active and passive wireless methods and energy harvesting.

TPMSs are categorized into two parts:

i. Indirect TPMSs
ii. Direct TPMSs

i. **Indirect TPMSs**

Indirect TPMs do not use existing pressure sensors. These measure the “apparent” air pressure, by monitoring individual wheel rotational speeds; and other signals available outside the tire itself. Most indirect TPMS use the measure that an underinflated tire has a slightly smaller diameter than a correctly inflated tire.

Newer developments of indirect TPMS can also detect simultaneous under-inflation in all four tires separately, using additional sensors for a vibration analysis of individual wheels or an analysis of load shift effects during acceleration. However, these additional sensors add to the complexity and cost of this technology. This study may not deal with the indirect TPMS as it needs the sensors to assign outside to monitor the tire speed or wheel speed.
ii. Direct-sensor TPMSs

Direct-sensor TPMSs use pressure measurements with wireless sensors attached inside or outside each tire. These sensors give the tires’ information or status to the vehicle’s user. These systems can be used for all of the tires of the vehicle by the means of a wireless sensor network. Here all tires of the vehicle constitute a node and all nodes are connected through wireless links with a system monitor. Direct-sensor TPMSs are designed to specifically cope with the effects of changes in tire pressure due to ambient temperature changes and road-to-tire friction, based temperature changes. Friction between the tire and road surface heats up the tire and increases its pressure. [10]

TPMSs are designed to provide drivers with tire pressure information and alerts needed to increase safety and save travel expenses through increased fuel efficiency, extended tire life, decreased downtime and maintenance, improved stability and handling; and decreased emissions. These are significant advantages and are summarized as follows:

- **Energy Savings**

  The TPMS helps to save energy in an efficient and effective manner. The under-inflated tires cause an increased rolling resistance of the tires on the road and consequently the vehicle’s engine must use more energy or petrol or gas to generate extra power to overcome that increased resistance, such as, a tire with 20% under-inflation reduces a 30% of the total mileage. With 50% under-inflation of a tire, there will be a 15% higher rolling resistance factor and 2-5% increase in the fuel consumption. The TPMS helps to minimize the under-inflation factors as well as to utilize the fuel consumption efficiently.

- **Decreased Downtime and Maintenance**

  Under-inflated tires lead to costly hours of downtime and maintenance.

- **Safety Assurance**

  TPMS improves the safe driving of vehicles on the road. Under-inflated tires lead to thread separation and tire failure which results in accidents, injuries; and deaths. Besides adding greater stability, better handling; and improving braking efficiencies, properly inflated tires provide greater safety for the driver, the vehicle, the loads; and others on the road.

- **Environmentally Friendly**

  The TPMS assists the decrease of CO₂ emissions into the environment. As under-inflated tires consume more petrol, it also results in increased combustion products and CO₂ emissions into the environment.

  In short, we can state that this dynamic monitoring and maintenance of tire-pressure by using WSNs is effective and increases safety by avoiding accidents. It is saving fuel by lower petrol consumption, extends tire life, decreases downtime and maintenance, improves stability and handling; and decreases emissions in the form of lower greenhouse gas emissions. Therefore, the choice of communication standard...
is important to support the sensor nodes. If the sensor nodes are supported during longer periods of time, the cost would come down as well as the harassment of reinstalling would decrease. Standards need to be chosen accordingly, considering those demands. Normally each vehicle’s driver is needed to check tire-status before any trip. So it is good if there exists a tire-pressure monitor in the vehicle that can show the status of the tires without manual checks. Here, the challenging factor is the battery power whether the sensor is inside or outside of a tire. [9][10][11]

2.4.6 Temperature Monitoring System

i. Automatic Temperature Control (ATC):

The temperature monitoring system is providing readings of the temperature of the vehicle inside and outside, using a WSN. According to these temperature readings, the user adjusts the inside temperature, which would offer a comfortable environment for them.

The ATC system consists of three major components (in addition to other assisting ones):

- ATC Controller – The core component which is referred to as the “brains” of the system
- Wireless Sensors – Supplying the pertinent input data to the controller
- Output Devices – Providing and displaying the result

According to MACS (Mobile Air Conditioning Society), the ATC controller is the core point which is referred to as the “brains” of the system. These controllers are essentially microprocessor devices. The ATC controller receives the data from the wireless sensors, processes them, and issues output commands to the various devices it controls. By being specialized, it has only one job: to do whatever it takes to keep the interior of the vehicle at a stable temperature. To improve the safety of the vehicle, the components might be equipped with an effective energy source, as well as a stable environment for the data processing which depends on the selected standard. [12]

ii. Engine Temperature Monitoring System (ETMS):

The ETMS is used for monitoring engine temperature and signal to the user when overheating occurs. This system shows the real-time engine temperature on the vehicle user’s interface. This system also needs an effective power source to work properly and to increase the safety of the vehicle. [12]

The ETMS consists of a set of wireless sensors. These sensors are dedicated to continuously read the temperature of the engine and report to the central unit which is monitored by the user on a display. If the engine overheats, the ETMS starts to give an alarm or warning intermittently. The ETMS needs support by a proper standard which will provide efficient power consumption for the long run as well as the capability to support other functionalities. The number of sensor nodes and their topology might be taken under consideration. By doing so, the driver will be able to
judge and act accordingly to decrease the temperature, whether by stopping for a moment or slowing down the car. This result reduces the likelihood of needing an engine replacement or reduces the repair cost.

The ETMS adds benefits in the following ways:

- Alerting driver when engine temperature is in critical stage.
- Preventing expensive engine repair cost.
- Real-time monitoring (on the display) of engine temperature.
- Reducing likelihood of engine overheating and stranding the driver.

### 2.4.7 Stall Removing System

Stall is the unexpected or unwanted stopping of an engine. To reduce this problem we can use a sensor which will help to locate the throttle. This sensor is named the Throttle Position Sensor (TPS). The throttle's position influences the timing of fuel injection and ignition. These timings are also dependent on the rate of change of the throttle’s position.

A TPS is usually used in the internal combustion engine of the vehicles and it is used for monitoring the position of the throttle. It is usually located on the butterfly spindle so that it can monitor directly the position of the throttle valve butterfly. It cannot be replaced very often. Therefore, to have a reasonable performance and to extend the durability of the TPS, the protocol or standard selection has to be considered carefully.
3 Wireless Technologies

3.1 IEEE 802.15.1

The standard IEEE 802.15.1 for WPAN is model after the Bluetooth specification and also published by the Bluetooth SIG. It is to be noted that Bluetooth has given rise to the era of Personal Area Network (PAN). Bluetooth is a low-power, short range radio technology and it is used for the replacement of wires for interconnecting devices such as keyboards, keyboards and mice. In addition, Bluetooth security is strong and robust and it uses the national standard AES algorithm for encryption.

The Bluetooth Special Interest Group (SIG) is a group of companies that cooperate to define Bluetooth standards and qualify Bluetooth products. The example of usage models for Bluetooth devices are – Wireless Headset, Internet Bridge, File Exchange, Synchronization, Printing, etc.

- Characteristics

Bluetooth operates in the unlicensed 2.4 GHz to 2.4835 GHz at a rate of 1 Mbps and employs Frequency Hopping Spread Spectrum (FHSS) technology for all transmissions. FHSS divides the frequency band into 79 channels. Bluetooth RF (physical layer) operation uses a Gaussian shaped, binary frequency shift keying (GFSK) modulation to minimize transceiver complexity; and a forward error correction (FEC) coding technique. Hopping of radio transceivers from one channel to another is determined by the master and it works in a pseudo-random manner. Bluetooth supports up to 8 devices (1 master and 7 slaves) in a piconet and piconet combines to form a scatternet.

- Network Topology

Depending on the application scenario, Bluetooth devices are of two types – master or slave. While several Bluetooth devices are trying to communicate, they have to synchronize to the same hopping sequence. The master device sets the hopping sequence, and the slave devices synchronize to the master device accordingly.

Two types of network:

i. Piconet – It is formed by a master and up to seven active slaves. Only the slaves communicate with the master. Every piconet consists of up to eight units.

ii. Scatternet - It is formed by linking two or more piconets. While a device is present in more than one piconet, it must time-share and be responsible to
synchronize to the master of the piconet with which it is currently communicating.

All units share the same frequency range within one scatternet. Within that scatternet, each piconet uses different hop sequences and transmits on different 1 MHz hop channels [13]. Bluetooth devices move in and out of range of one another, therefore, the networks are constantly being formed, modified; and dissolved.

Figure 3.1 Topology of: a piconet with one slave device (a); a piconet with several slave devices (b); a scatternet (c). [14]

➢ Service Discovery

When a Bluetooth device required a service from others, initially, it needs to determine what kind of Bluetooth devices are present and what services they desire or offer. Therefore, service of discovery is utilized and this feature begins by sending out a query for other Bluetooth devices and the information needed to establish a connection with them. While the successful attempts ensure by finding other Bluetooth devices and establishing communication with them, the Service Discover Protocol (SDP) is utilized to determine what services are supported and what kind of connections should be made.

➢ Power Level and Range

Most of the Bluetooth devices are dependent on batteries for energy. Considering the energy factor, Bluetooth devices are of the following classes:

<table>
<thead>
<tr>
<th>Devices</th>
<th>Energy</th>
<th>Energy Level</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class 1</td>
<td>Low</td>
<td>0 dBm or 1 mW</td>
<td>Up to 1 meter (3 feet)</td>
</tr>
<tr>
<td>Class 2</td>
<td>Medium</td>
<td>4 dBm or 2.5 mW</td>
<td>Up to 10 meter (33 feet)</td>
</tr>
<tr>
<td>Class 3</td>
<td>High</td>
<td>20dBm or 100 mW</td>
<td>Up to 100 meter (328 feet)</td>
</tr>
</tbody>
</table>

Table 3.1 Bluetooth device transmitter classes
Bluetooth class 2 and 3 devices can optionally implement adaptive power control. Required for class 1 devices, this mechanism allows a Bluetooth radio to reduce energy consumption to the minimum level required to maintain its link, thus saving energy and reducing the potential for interfering with other nearby networks. [15] [16]

➤ Security Features

The basic security services of Bluetooth are mentioned as follows [16]:

i. Authentication
   Identification of the communicated devices is verified by using the addresses of the involved Bluetooth devices. Bluetooth does not provide the authentication of the native users.

ii. Confidentiality
   Only authorized devices can access and view transmitted data. It ensures the prevention of information from the effect of eavesdropping.

iii. Authorization
   Only authorized devices are permitted and given preferences to use a requested service.

➤ Protocols based on IEEE 802.15.1

3.1.1 Bluetooth

Bluetooth is meant to be a cable replacement. It operates in the 2.4 GHz ISM band and uses frequency hopping for preventing interference. The data rate is up to 3 Mbps and maximum range is up to 100 meter.

3.1.2 WISA

WISA (Wireless Interface for Sensors and Actuators) is based on the IEEE 802.15.1 physical standard. It operates at 2.4 GHz frequency and transfer rate is 1 Mbps. It is real time capable because of its deterministic time behaviour. It uses frequency hopping to prevent the interference of other networks. WISA has 360 devices per cell and maximum of 120 devices per master. Two systems of WISA (as WISA-COM and WISA-POWER) can be combined. WISA-COM is only for the wireless communication and WISA-POWER is for the communication and power supply via RF similar to RFID and anti-theft devices

3.2 IEEE 802.15.3/UWB

Ultra-wide-band (UWB) uses very low powered and short pulse radio signals to transfer data over a wide spectrum of frequencies. It is tolerant to disturbances because of its broad spectrum of frequencies, it is therefore more suitable for a noisy...
automotive environment. Among the WPAN standards, UWB offers a much higher bandwidth than the dominant Bluetooth. Network speed of UWB is up to 100 Mbps. [17]

### 3.3 IEEE 802.15.4

Throughout this chapter, the architecture of IEEE 802.15.4 with the explanation of IEEE 802.15.4 fundamentals (i.e., node types or its devices) are studied as well as the network topologies, followed by IEEE 802.15.4 MAC design and its services.

- **Fundamentals of IEEE 802.15.4 Design**

According to [18], IEEE 802.15.4 has several components. The most important are its devices. The devices can be classified mainly in two categories.

1. **FFD (Full-Function Device)**
2. **RFD (Reduced-Function Device)**

#### i. FFD

A network should have at least one FFD which operates as PAN (Personal Area Network) coordinator.

FFD operates in three modes. Such as:

- PAN coordinator
- A coordinator
- A device

An FFD has all the functionalities such as talking to FFDs and also RFDs. FFDs can send large amounts of data. FFD are used in both complex and simple applications.

#### ii. RFD

RFDs are simple devices with very simple resource and communication requirements. RFDs only talk to FFDs. RFDs never act as a PAN coordinator and cannot support sending a large amount of data. RFDs are only used for applications which are extremely simple.

- **Characteristics of IEEE 802.15.4**

The standard IEEE 802.15.4 for WPAN defines the physical and MAC layer and this standard can physically operate in the three free Industrial, Scientific and Medical (ISM) frequency bands. It offers a license free spectrum at 868.0-868.6 MHz in Europe, at 912-928 MHz in North America and at 2,400-2,483.5 MHz worldwide. In the worldwide 2.4 GHz band, 14 overlapping chirp spread spectrum (CSS) channels added to the IEEE 802.15.4 standard. IEEE 802.15.4 has some versions such as IEEE 802.15.4-2003 (mostly called IEEE 802.15.4), IEEE 802.15.4-2006 and IEEE 802.15.4a-2007. The addition of ASK and O-QPSK modulation which enables a higher transfer
rate at the lower frequencies is the main difference between IEEE 802.15.4 and IEEE 802.15.4-2006.

- **Topologies of IEEE 802.15.4**

IEEE 802.15.4 supports three types of topologies. [19] Such as:

- Star topology
- Peer-to-peer topology
- Cluster tree

**Star Topology**

In the star topology, a single central controller is surrounded, i.e., communicated to by several devices, where the central controller is called PAN coordinator and the other nodes are supporting devices. The PAN coordinator is externally powered (alternating current, AC electric power supply) and rarely battery powered. The supporting devices are mostly likely to be battery powered. Applications that benefit very much from this topology are home automation, games or personal computer peripherals and so on.

In this topology, FFD is activated first. After its activation, it establishes its own network and becomes the PAN coordinator. Then every star network chooses its PAN identifier which is not used by any other networks. Only this feature helps the star network to act and operate individually.

![Figure 3.2 Star Topology](image)

**Peer-to-peer Topology**

In this topology, one PAN coordinator is available as in the star topology. The big difference between the star and a peer-to-peer topology is that in a peer-to-peer topology any device can communicate with any other device if they are in range of one another. Another important feature for this topology is that it can be ad hoc, self-healing and self-organizing.

Applications that would be very much benefited by this topology are industrial monitoring and control, inventory and asset tracking. Multiple hops make routing
messages necessary as this feature helps to convey the message from one device to any other device in the network. Reliability is ensured by this multipath routing.

Figure 3.3 Peer-to-peer Topology

- **Cluster-tree Topology**

In the cluster-tree topology, most of the devices are FFDs. An RFD connects to a cluster-tree network as a leaf node at the terminal end. It is a special kind of peer-to-peer network. Among the FFDs, any of them can act as a coordinator and provide synchronization services to other devices and coordinators, and only one of these coordinators is the PAN coordinator. This topology covers larger area than the other ones.

Figure 3.4 Cluster-tree topology
Operational Modes

IEEE 802.15.4 uses a protocol which is based on the CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) algorithm. This algorithm is the modified version of CSMA and makes the transmission over the channel with more efficiency than CSMA. When a node wishes to transmit data, it has to first listen to the channel for a predetermined amount of time to determine whether another node is transmitting over the channel or not. This reduces the probability of collision with other ongoing transmissions. [20]

IEEE 802.15.4 personal area networks (PAN) have the following two operational modes depending on the latency requirements:

- Non-beacon-enabled Operational Mode
- Beacon-enabled Operational Mode

- Non-beacon-enabled Operational Mode

In this operational mode, nodes are using an un-slotted CSMA/CA protocol to access the channel and transmit their packets. This algorithm uses a back-off period to space out repeated retransmissions of the data.

In non-beacon-enabled operational mode, nodes are transmitting in two different states:

- While the channel is free: Each node will wait for a random number of back-off periods before transmitting. After this interval, for one unit of time channel sensing is performed by the node. If the channel is found free, the node immediately starts the transmission.

- While the channel is busy: In this case, the node has to enter the back-off state again. A maximum number of times for sensing the channel by a node are specified. When the maximum number of times for sensing the channel is reached by the node, the algorithm quits and the transmission is stopped.

- Beacon-enabled Operational Mode

In this operational mode, the super-frame is introduced. It manages channel access and it is bounded by the transmission of the beacon frame or packet. The super-frame starts with the beacon packet which is transmitted by the WPAN coordinator. The beacons are responsible to synchronize the attached devices, to describe the structure of the super-frame, and to identify the network. Network devices communicate with the PAN coordinator and the communication occurs in the period between two successive beacons. The beacon period is variable in binary multiples of 15.36 ms, up to a maximum of 15.36 ms * 2^14 = 4 minutes 11.66 seconds. This variability of period time supports the optimum trade-off for each application between the network node power consumption and message latency.

Super-frame Structure:

The super-frame has two different parts (see figure 3.5):
i. Inactive part

ii. Active part

i. Inactive part

The inactive part allows the nodes to go into sleeping mode or low-power mode in order to save energy. During this part, the devices shall not interact with the PAN and may enter in the mentioned low-power mode.

ii. Active part

The coordinator interacts with its network only during the active part of the superframe. The active part has two different parts such as

- **Contention Access Period (CAP)**

  Channel access is contention based by using the CSMA/CA mechanism. The beacon is followed by a CAP for devices attempting to gain access to the channel. The length of CAP is adjustable as a fraction of the period between two beacons.

- **Contention Free Period (CFP)**

  CFP is optional and composed of Guaranteed Time Slots (GTS). The PAN coordinator can assign dedicated portions of the super-frame to a specific network device requesting it. These segments of time are called GTS. The format of GTS is shown in figure 3.6. It contains three subfields and is one byte long. The three subfields are called GTS Length, GTS Direction and Reserved (see figure 3.7). GTS Length contains the number of GTS slots being requested by the device and GTS Direction defines for the data flow from the device (here GTS is owned by the device) whether the device is the receiver or transmitter. If the GTS Direction is 1, it is a receiver-only GTS and if it is set to zero, it is a transmitter-only GTS. A GTS is allocated by the PAN coordinator to the specific nodes to address the special needs of applications requiring low message latency and bandwidth. It reserves channel time for individual devices without using the access mechanism of CSMA/CA.

In fig-3.5, we can see that the active portion of a super-frame is divided into 16 equally spaced slots which are also called super-frame slots.

In the CAP, all data transmissions rely on a slotted Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA) algorithm. For a single super-frame, a maximum of seven GTSs is allocated and GTS transfer mode is only applicable in star networks. [21] [22]

![Superframe Structure in general](image)

Figure 3.5 Superframe Structure in general
Super-frame Duration (SD): Total time of CAP, CFP (GTS) and beacon which does not include the inactive period

Beacon Interval: Time between two successive beacons

For our WSN in-vehicle applications, the beacon-enabled operational mode should be an appropriate design choice, because of the synchronization and the latency guarantee. Synchronization is maintained by the PAN coordinator which transmits periodic beacons. The design will also provide latency guarantees using the collision-free GTSs in the CFP.

- Calculation of beacon order and super-frame order:

The structure of the super-frame structure is determined by two parameters:
- Super Order (SO) is the variable which determines the length of the Super-frame Duration (SD)
- Beacon Order (BO) determines the length of the Beacon Interval (BI)

For both BO and SO we have:
\[ 1 \leq SO \leq 15 \]
\[ 1 \leq BO \leq 15 \]

Where are
- BO = 15 indicates that there are no beacon transmissions.
- SO = BO indicates that the super-frame duration is same as the beacon interval, which indicates that no inactive portion is available.
• BO > SO indicates that an inactive portion is present in the super-frame. [23] [24] [25]

For (BO) and (SO), the following has to hold true:

$$BO \geq SO$$

The duration of the active part and the whole super-frame is depended on the SO and BO value which ranges from 0 to 14 (when assuming beacon transmissions).

$$0 \leq SO \leq BO \leq 14$$

- **Calculation of duty cycle:**

  Duty cycle = \(2 (SO - BO) \times 100\)

  The duty cycle is always represented as in percentage

- **Power Consumption and Security Considerations**

  The IEEE 802.15.4 MAC sub layer is very suitable for battery-powered devices as battery-powered devices require duty-cycling to reduce power consumption. These devices spend most of their operational life in sleep mode, but each device periodically listens to the RF channel in order to determine whether a message is pending or not. The decision on the balance between battery consumption and message latency is done by the help of this mechanism.

  The IEEE 802.15.4 MAC sub layer provides basic security services and interoperability among all the devices implementing this standard. This baseline includes the ability to maintain an access control list (ACL) and the usage of symmetric cryptography to protect transmitted frames. The ability to perform this security functionality does not imply, however, that it should be used at any given device. When security functions are to be used at the MAC sub layer is determined by the higher layers. The standard needs to demonstrate these power consumption and security features by the means of simulation. [26]

- **Protocols based on IEEE 802.15.4**

  Several protocols based on the IEEE 802.15.4 are taken under consideration in the following manner [27]

  **3.3.1 ZigBee**

  ZigBee is a low-power and low-cost wireless sensor network standard. Usually, it is used in energy management and efficiency, also industrial automation as well as home and building automation. This standard uses the IEEE 802.15.4 standard and ZigBee has some features in addition to those of IEEE 802.15.4. The first two layers of OSI model, physical (PHY) and medium access (MAC), are defined by IEEE 802.15.4 standard and the layers above them are defined by ZigBee. This protocol uses the IEEE 802.15.4 standard and operates with 250 Kbps in 2.4 GHz frequency. As the nodes can be in sleep mode for most of the time, ZigBee is acceptable for the low power communication which has a low duty cycle (i.e. less than 0.15%). The
maximum range of this network is up to 200 meter and maximum number of supported nodes is 1024. The ZigBee modules which have a range more than 1000 m operate with the maximum allowed transmit power of 10 mW. For security purposes, ZigBee can use 128 bit AES encryption.

### 3.3.2 6LoWPAN

6LoWPAN (IPv6 over Low power Wireless Personal Area Network) is designed to be used for energy management in home and building automation. This protocol operates with 250 Kbps data rate in the 2.4 GHz frequency range only. The range of a network is up to 200 meters and the maximum number of nodes is 100. 6LoWPAN protocol has not defined any encryption method.

### 3.3.3 Wireless HART

Wireless HART protocol is used for industrial applications for process monitoring and regulation. This protocol uses the IEEE 802.15.4-2006 standard in the free frequencies around 2.4 GHz. This protocol also uses frequency hopping for preventing interference from other applications. The range of a network is up to 250 meter and uses 128 bit AES encryption.

### 3.3.4 ISA 100

ISA 100 is used for industrial automation. It uses the IEEE 802.15.4-2006 standard in the 2.4 GHz frequency band. It also uses frequency hopping for preventing interference from other wireless networks. The most important property of ISA 100 is the low latency or fast response time which is 100 ms.

### 3.3.5 EnOcean

EnOcean works in the frequencies of 868 MHz for Europe and 315 MHz for North America. The transmit range is up to 30 meters inside the buildings and up to 300 meters outside the buildings. Available modules of Battery less EnOcean with energy harvesting reduce lifecycle cost as they are free of maintenance.

### 3.3.6 WiMi

WiMi works in 2.45 GHz frequency and it has two standards (WiMi and WiMi P2P) based on IEEE 802.15.4-2003. The protocol is suitable for short messages to communicate with the sensors. Both of the standards of WiMi have a range up to 125 meters indoors and up to 550 meters outdoors. The maximum number of nodes for this type of network is 1024 and the communication can use 32, 64 or 128 bit AES encryption.
3.3.7 SimpliciTi

SimpliciTi is based on the IEEE 802.15.4 standard and works in the 433 MHz, 868 MHz and 915 MHz frequencies. The data rate is up to 300 kbps and range is at 100 meters.

3.4 ANT

ANT is a wireless protocol used for industrial and home automation and logistics or goods tracking. It operates in the 2.4 GHz frequencies and is optimized for short package transmission. It allows a burst transfer rate up to 20 kbps and the maximum number of devices per channel is limited to 65533. [27]

3.5 WiFi

Wireless Local Area Networks (WLANs) also known as WiFi is based on the IEEE 802.11 standards and depending on local authority restrictions IEEE 802.11 b/g/n supports up to 14 channels in the 2.4 GHz frequency range. WiFi is a well-established network, wide spread and used in various environments and devices. The transfer rate is up to 11 Mbps for IEEE 802.11b, up to 54 Mbps for IEEE 802.11g and up to 72 Mbps for IEEE 802.11n using a single stream on a single channel. Direct Sequence Spread Spectrum (DSSS) for IEEE 802.11b, Orthogonal Frequency Division Multiplexing (OFDM) for IEEE 802.11g/n are used as modulation technique of IEEE 802.11. Though such verities are available, access points always announce its network with beacon frames and beacon frames are usually sent with the lowest data rate of 1Mbps to 2 Mbps for comparability reasons. Same CCA modes as WSNs are supported by WiFi. [28]

3.6 Z-Wave

Z-wave uses low power RF radio for low power remote control applications. Z-wave Alliance standardizes this technology. Z-wave operates in sub 1 GHz band. As 2.4 GHz RF band is subject to significant interference due to IEEE 802.11 and IEEE 802.15.1 devices, it has a better with respect to IEEE 802.15.4. It is also to be noted that 868 MHz ISM band used by Z-wave is limited to European regulations to operate at or below 1% duty cycle whereas 1% duty cycle operation in the band could be enough for most of the control applications. The range is 30 meters at a maximum transfer rate of 40 kbps and the transceivers from Zensys allow 100 meters of outdoor range. A maximum of 232 nodes in the network is allowed and mesh topologies could be formed as well. [17]
Chapter 4

4 Design Choice for Wireless Communication

4.1 Operation Modes

Wireless networks have two modes of operation [31]:

i. Ad hoc

An ad hoc wireless network does not need to have a base station. Self organization is the key feature of this type of network while there is no base station/central node to talk to. The wireless terminals may communicate directly with each other.

ii. Infrastructured

Infrastructured wireless networks must have a base station. The base station of this type of network acts as a central node and connects the wireless terminals. The base station provides the features to enable access to other wireless networks or internet or intranet and wireless terminals use the base station to relay their messages. Usually the base stations are located in a fixed point, though mobile base stations also exist.

The drawback of the infrastructured wireless network is the failure of the centre point. If the centre point fails, the wireless terminals cannot communicate with each other.

<table>
<thead>
<tr>
<th>Standard</th>
<th>Ad hoc</th>
<th>Infrastructured</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 802.15.1</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>IEEE 802.15.4</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>IEEE 802.11a/b/g/n</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 4.1 Modes of operation of different IEEE standards

Table-4.1 states that the discussed wireless standards (IEEE 802.15.1, IEEE 802.15.4, IEEE 802.11) only perform in the Infrastructured operational mode, whereas IEEE 802.11 performs in Ad hoc operational mode also.
4.2 Medium Access

In which procedure the wireless terminals will access the medium must be established for the sake of wireless communication. A protocol is responsible to establish the fact of accessing. CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) technique allows wireless transmissions to be completed without interference from other terminals and it is used by several IEEE standards.

While CSMA/CA is used, a part of the potential data rate is lost to the overhead of this protocol. For the one-way communication, channels could be better utilized, as the source terminal would not have to take into consideration transmissions being sent from other terminals. In case of the problems of hidden terminal, Request to Send/Clear to Send (RTS/CTS) scheme could be used to reserve the channel for the communication.

4.3 Frequency, Data Rate and Range

IEEE standards use different frequencies and therefore, different frequencies affect the data rate and range covered by them. It is to be noted that shorter range communication has lower power requirements as well as enabling equipment to be smaller and the potential for frequency reuse is very good, also vice versa.

<table>
<thead>
<tr>
<th>Standard</th>
<th>Frequency</th>
<th>Data Rate</th>
<th>Range</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 802.11g/n</td>
<td>2.4/5 GHz</td>
<td>54 Mbps, 248 Mbps</td>
<td>140 m/250m</td>
<td>LAN</td>
</tr>
<tr>
<td>IEEE 802.15.1</td>
<td>2.4 GHz</td>
<td>3 Mbps²</td>
<td>100 m</td>
<td>PAN</td>
</tr>
<tr>
<td>IEEE 802.15.3</td>
<td>3.1-10.6 GHz</td>
<td>100 Mbps</td>
<td>30 m</td>
<td>PAN</td>
</tr>
<tr>
<td>IEEE 802.15.4</td>
<td>868/915 MHz, 2.4 GHz</td>
<td>40 kbps, 250 kbps</td>
<td>75 m</td>
<td>PAN</td>
</tr>
</tbody>
</table>

Table 4.2 Comparison of different wireless standards [31]

Here, LAN is for Local Area Network  
PAN is for Personal Area Network  
BAN is for Body Area Network  
Data rate is for outdoor environments with few obstructions  
¹ IEEE 802.11n device with two streams (four antennas)  
² Bluetooth versions 2.0  
³ Bluetooth class 1 device

The above Table-4.2 represents that most of the wireless standards use the free license (ISM) 2.4 GHz frequency range except IEEE 802.15.3 which uses the 3.1-10.6 GHz frequency range and it has highest data rate (100 Mbps) among them. The design of IEEE 802.11g is designed to be compatible with IEEE 802.11b so that they can co-exist. Whenever IEEE 802.11g base station operates in IEEE 802.11b mode, its data rate is reduced to that of IEEE 802.11b for all its connected terminals. If one standard uses the same frequency band but a different signalling method, it does not suffer too badly from interference. As for example, IEEE 802.15.1 uses the same
frequency band (2.4 GHz) with IEEE 802.11b/g but uses a different signalling method.

Within the same frequency, the data rate of one standard could be higher than the other standard. Large data rate and range can be achieved by using the technique MIMO (Multiple-Input Multiple-Output) where more than one sender and receiver antennas are used and combine this with special coding techniques in order to squeeze even more data through the same frequencies.

### 4.4 Modulation and Signal Coding

For transmitting binary data over the wireless medium, digital-to-analogue (D/A) modulation is needed. After receiving the analogue signal, it needs to be converted back into the digital form for retrieving the binary data.

The modulation technique for a standard will be chosen on two factors:

i. Based on the design goals of the standard.
ii. The target environment where it will be deployed.

Every technique has different characteristics and different strategies:

- Power consumption
- Noise resistance (fading, multi path, etc.)
- Spectral efficiency (efficient frequency use)
- Hardware complexity

<table>
<thead>
<tr>
<th>Technique</th>
<th>IEEE 802.11n</th>
<th>IEEE 802.15.1</th>
<th>IEEE 802.15.3</th>
<th>IEEE 802.15.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSK</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>FSK</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ASK</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>QAM</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CCK</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alamouti</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>OFDM</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SS</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

Table 4.3 Modulation and coding techniques of different standards [31]

The table has shown the usable modulation and coding scheme of the different standards. It is also to be noted that not all the schemes are mandatory for each standard as for example, PSK is used by all the wireless standards except IEEE 802.11n. In the case of interoperability requirements, some of the standards may be required while others are entirely optional. This interoperability feature depends on which revision of the standard is used.

The elaboration of the modulation and coding schemes used by the standards are as follows:

- PSK (Phase-Shift Keying)
- Binary Phase-Shift Keying (BPSK)
- Quadrature Phase-Shift Keying (QPSK)
- Offset Quadrature Phase-Shift Keying (OQPSK)
- Differential Phase-Shift Keying (DPSK)

- FSK (Frequency-Shift Keying)
  - Gaussian Frequency-Shift Keying (GFSK)
- ASK (Amplitude-Shift Keying)
- QAM (Quadrature Amplitude Modulation)
- CCK (Complementary Code Keying)
- STBC (Alamouti Space-Time Block Coding)
- OFDM (Orthogonal Frequency-Division Multiplexing)
- SS (Spread Spectrum)
  - DSSS (Direct-Sequence Spread Spectrum)
  - PSSS (Parallel-Sequence Spread Spectrum)
  - AFH (Adaptive Frequency-Hopping Spread Spectrum)

IEEE 802.11a/b/g uses 64-QAM and this standard manages to map 6 data bits into each transmitted symbol. This is, therefore, called “High order modulation” and while combining with OFDM, it provides a high spectral efficiency.

While using 64-QAM instead of BPSK and QPSK, signal demodulation requires a higher signal to noise ratio (SNR) for the receiver. This is the disadvantage of using 64-QAM. It is clear in a general sense that high order modulation requires a higher transmit power. Lower order modulation (such as BPSK and QPSK) requires a lower transmit power, as for example, IEEE 802.15.4 uses BPSK and OQPSK (similar to QPSK). The reason to choose BPSK and OQPSK is the design goal of IEEE 802.15.4. The design goal of IEEE 802.15.4 is to create devices with low power consumption and therefore, it needs to reduce the power requirements to a minimum. Spectral efficiency is the scale to measure the transmission speed of data in a predefined bandwidth. The unit of spectral efficiency is bits/s/Hz and every modulation techniques have its own measurement. In case of noise resistance, every modulation methods are more or less immune to noise. More noisy environment requires more signal power for a given noise level. Amplitude modulation (AM) is far more susceptible to noise so they have a higher BER for a given modulation whereas phase and frequency modulation (BPSK, FSK, etc.) fare better in a noisy environment. [31]

### 4.5 Energy Consumption

While sensors are inactive, the transceivers can switch into sleep mode which uses the lowest energy. The duration of this mode varies on the application and can vary from seconds, minutes to hours. The more the duration of sleep mode, this provides the more efficiency in energy consumption. If the batteries are involved as an energy source in some sensors, it is important to have very low energy consumption, as the cost to change the batteries will be more than the battery itself. In this case, data rate and latency are not important and can be of lower performance. In the following, Table-4.4 represents the energy consumption of IEEE 802.15.4, Bluetooth and Wi-Fi
in several (sleep, receive and transmit) states. In every state, Wi-Fi is consuming the most and ZigBee consuming the least.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Energy Consumption</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sleep</td>
</tr>
<tr>
<td>ZigBee</td>
<td>0.06 µW</td>
</tr>
<tr>
<td>Bluetooth</td>
<td>330 µW</td>
</tr>
<tr>
<td>WiFi</td>
<td>6600 µW</td>
</tr>
</tbody>
</table>

Table 4.4 Energy consumption of several wireless standards [27]

ZigBee and Bluetooth are used for short ranges and limited energy sources, which leads to very low energy consumption. UWB is used for short range and high data rate applications. Wi-Fi is for longer connection and support devices with a substantial energy source. For comparing the energy consumption of wireless protocols, we want to consider their publicly available chipsets.[30][35]

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Blue Tooth</th>
<th>ZigBee</th>
<th>Wi-Fi</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chip set name</td>
<td>RN-42</td>
<td>CC2520</td>
<td>XG-180M</td>
</tr>
<tr>
<td>Voltage (V)</td>
<td>3.3</td>
<td>3</td>
<td>3.3</td>
</tr>
<tr>
<td>Transmission Speed (kbps)</td>
<td>723.2</td>
<td>250</td>
<td>54000</td>
</tr>
<tr>
<td>Tbit (us)</td>
<td>1.38</td>
<td>4.00</td>
<td>0.02</td>
</tr>
<tr>
<td>Delay, Low Power -&gt; Active (us)</td>
<td>5000</td>
<td>200</td>
<td>75000</td>
</tr>
<tr>
<td>Delay, Active -&gt; Transmit (us)</td>
<td>0</td>
<td>192</td>
<td>210</td>
</tr>
<tr>
<td>Low Power Current Usage (mA)</td>
<td>0.026</td>
<td>0.175</td>
<td>0.2</td>
</tr>
<tr>
<td>Active Current Usage (mA)</td>
<td>40</td>
<td>1.6</td>
<td>10</td>
</tr>
<tr>
<td>Transmit Current Usage (mA)</td>
<td>40</td>
<td>25.8</td>
<td>450</td>
</tr>
</tbody>
</table>

Table 4.5 Energy consumption of chipsets for each protocol

In Table-4.5, we have considered chipsets as RN-42, CC2520, XG-180M for Bluetooth, ZigBee and Wi-Fi respectively. Related parameters have been mentioned according to the respective chipset. We will use those parameters’ values to get the energy consumption per bit.
According to the above-mentioned data of the tables we can do the following transmission and energy calculation.

The calculation of the transmission time, $T_{tx}$ is [35]:

$$T_{tx} = (N_{data} + \text{ROUNDUP}(N_{data}/N_{maxPld}) \times N_{ovhd}) \times T_{bit} + T_{prop}$$

The energy consumption is calculated according to the following formula [35]:

$$E = [A_{lp}(T_{hold} - T_{lp\_active} - T_{active\_tx}) + \text{AVG}(A_{lp}, A_{active}) \times T_{lp\_active} + \text{AVG}(A_{active}, A_{tx}) \times T_{active\_tx} + A_{tx} \times T_{tx}] \times V_{cc}$$

Where,

- $T_{tx}$ = transmission time
- $N_{data}$ = data size
- $N_{maxPld}$ = Max payload length
- $N_{ovhd}$ = Max overhead
- $T_{bit}$ = Bit time
- $T_{prop}$ = Propagation time
- $E$ = Energy
- $A_{lp}$ = Low power current consumption
- $A_{active}$ = Active current consumption
- $A_{tx}$ = Transmission current consumption
- $T_{hold}$ = Hold time
- $T_{lp\_active}$ = Low power to active transition delay
- $T_{active\_tx}$ = Active to transmit transition delay
- $T_{tx}$ = Transmission time
- $V_{cc}$ = Source voltage of the chip

According to the calculation, Bluetooth, ZigBee and Wi-Fi device consume 0.342 mJs$^{-1}$ (0.0214 mJs$^{-1}$/bit), 0.067 mJs$^{-1}$ (0.0042 mJs$^{-1}$/bit) and 1.4385 mJs$^{-1}$(0.09 mJs$^{-1}$/bit).
respectively when transferring 2 bytes (16 bits) of data. Moreover, Bluetooth, ZigBee and Wi-Fi device consume 1.531 mJs\(^{-1}\) (0.000383 mJs\(^{-1}\)/bit), 4.248 mJs\(^{-1}\) (0.00106 mJs\(^{-1}\)/bit) and 4.8 mJs\(^{-1}\) (0.0012 mJs\(^{-1}\)/bit) respectively when transferring 500 bytes (4000 bits) of data in 5000 ms.

Bluetooth and ZigBee perform for short ranges and limited battery power. They offer very low energy consumption and, in some cases, will not measurably affect battery life whereas Wi-Fi is designed for a longer connection and supports devices with a substantial energy supply.

4.6 Security

- **Security Analysis of IEEE 802.11**

The two approaches of security in the IEEE 802.11 are highlighted as follows [32]:

**A. Wired Equivalent Privacy**

WEP was the first approach to offer security in the IEEE 802.11 standards and it is proved that it was a poor effort and implementation from the vendors, especially in its design flaws. Therefore, it failed to provide security in an expected manner and several successful attacks referred its weaknesses.

**B. IEEE 802.11i**

Having awareness and recovering the failures of WEP, Wi-Fi Alliance presented Wi-Fi Protected Areas (WPA) which is originally called WEP2. It has Integrity Handling (TKIP), and Key Management (802.1X) as well as the symmetric cipher (AES), and secure de-authentication/dis-association. The Wi-Fi Alliance announced the WPA2 as the new specifications dictated by IEEE 802.11i.

IEEE 802.11i defines a Robust Security Network Association (RSNA) where RSNA helps the IEEE 802.11 to provide function to protect data frames, IEEE 802.1X provides authentication and a Controlled Port, and 802.11 and 802.1X collaborate to provide key management.

IEEE 802.11i mainly defines a number of security features in addition to WEP and IEEE 802.11 authentication which includes:

- Enhanced authentication mechanisms for Stations.
- Key management algorithms.
- Cryptographic key establishment.
- An enhanced data encapsulation mechanism, called CTR with CBC-MAC Protocol (CCMP).
- Optionally, Temporal Key Integrity Protocol (TKIP).

Authentication and Confidentiality are the two security services provided by IEEE 802.11.
For authentication, an RSNA uses 802.1X authentication service with TKIP and CCMP whereas for Confidentiality and Data Integrity, RSN key management with TKIP and CCMP are used.

- **Authentication:** 802.11 define three authentication methods: Open System, Shared Key, and RSNA. Open System Authentication admits any station to the Distribution System (DS: A system used to interconnect a set of basic service sets (BSSs) and integrated LANs to create an extended service set (ESS)). Shared Key Authentication relies on WEP to demonstrate knowledge of the WEP encryption key. An RSNA supports authentication based on 802.1X, or pre-shared keys (PSK). 802.1X uses Extensible Authentication Protocol (EAP) to authenticate stations and the Authentication Server (AS).

- **Confidentiality:** 802.11i accepts three different cryptographic algorithms to protect traffic information: WEP, TKIP, and CCMP. WEP and TKIP use RC4 as the encryption engine. CCMP is based on the Advanced Encryption Standard (AES).

- **Key Management:** The enhanced authentication, confidentiality, and replay protection mechanisms demand fresh cryptographic keys. The keys are distributed using 4-Way Handshake and Group Key Handshake protocols.

- **Data Origin authenticity:** Data Origin Authenticity mechanisms mean a station can verify which station sent the MAC Protocol Data Unit (MPDU). This is to prevent possible masquerading attacks. This service is provided using CCMP or TKIP.

- **802.1X & EAP:** 802.1X is a protocol that enables port-based authentication. All stations have associated ports; and all traffic is blocked in the station port until the client gets authenticated by an Authentication Server (AS). Extensible Authentication Protocol (EAP) was created originally as an extension to the Point-to-Point Protocol used in dial-up connections and it defines a generalized framework for multiple authentications.

- **Pre-Shared Key:** In small wireless networks like SOHO’s, the deployment of an 802.1x infrastructure for key distribution is overkill and not practical and therefore, 802.11i introduces a special mode of key distribution called Pre-Shared Key (PSK). In this mode, a shared secret key called Master Key must be entered manually in all AP; and all clients.

- **Security Methods:** 802.11i defines Pre-RSNA and RSNA security methods.
  
  Pre-RSNA methods are implemented by the following algorithms:
  
  - WEP
  - 802.11 entity authentication

  RSNA security is provided by the following algorithms:
  
  - TKIP
  - CCMP
  - RSN
The establishment and termination procedures, includes 802.1X authentication.

• Key management procedures

➢ **Entity Authentication:** In an ESS, a station and an AP must complete an 802.11 authentication before an association. This exchange is optional in an IBSS. 802.11i defines two authentication methods.
   - “Open System Authentication”
   - “Shared Key Authentication” authenticates stations that share a common known key.

➢ **Temporal Key Integrity Protocol (TKIP):** 802.11i states that implementation of TKIP is optional. TKIP offered a fix for the main problems related with WEP. Its main purpose is to be applied to existing hardware via software upgrades; and offers backward compatibility with major hardware existing.

➢ **CCMP:** 802.11i states that implementation of CCMP is mandatory for devices claiming to be RSNA compliant. CCMP stands for CTR (Counter mode) with CBC-MAC (Cipher-Block Chaining with Message Authentication Code) Protocol. It provides authentication, confidentiality, integrity, and replay protection. All AES processing used within CCMP uses AES with a 128-bit key and a 128-bit block size.

➢ **RSNA Security Associations Management:** Security Associations are used to guarantee secure communications; and these associations provide information about the cipher solutions to be used. A Security Association is the set of policies, keys; and parameters used to protect information. The information in the security association must be stored in each entity that will use the association; and has to be consistent with all parties.

➢ **Key Management procedures:** RSNA defines two hierarchies of keys:
   - Pairwise key hierarchy to protect unicast traffic.
   - GTK to protect multicast or broadcast traffic.

802.11i is a more consciously designed security protocol with authentication, identity and confidentiality which includes per-port authentication (802.1X) and can be implemented to support highly sophisticated authentication schemes like per-user authentication using PKI (EAP). It offers a strong solution for security in wireless networks with a strong encryption algorithm (AES-CCMP), and supports per-MPDU authentication, integrity; and replay control.

➢ **Security Services of IEEE 802.15.1**

The Bluetooth technology can be used to design and implement a lot of applications. Therefore, this technology is complicated and cumbersome while security is a matter of concern. At present, Bluetooth defines security at the link level. Application level security is not specified and it is up to the application developers to select the most appropriate security mechanisms. Currently, higher functionality is demanded through this technology than higher security and robustness. However, including the security and robustness of the applications of IEEE 802.15.1 is dependent on the designer. [32]
Security Services of IEEE 802.15.4

The IEEE 802.15.4 address the security services through the link-layers security package and applications sitting on top of the link layer must specify the security requirements. By default, the security is not enabled. Link layer security protocol offers the following services [32]:

- Access control.
- Message integrity.
- Message confidentiality.
- Replay protection.

A. Access Control

Access Control means the security protocol should prevent unauthorized parties from participating in the network and IEEE 802.15.4 offers this security service.

B. Message Integrity

Message Integrity means that legitimate nodes should detect if a message comes from an authorized node and if not, reject them. A message authentication code is a cryptographically secure checksum of the message and it helps to provide message authentication and integrity.

C. Message Confidentiality

Confidentiality means to keep the information secret from any unauthorized parties and this security service is usually provided by encryption schemes. The encryption scheme should prevent message recovery and also prevent the learning of partial information from the encrypted message. This type of security is known as semantic security. Cipher text is one of the implications of that semantic security which imposes by encrypting the same plaintext two times.

D. Replay protection

Replay Protection is a security service where the sender will assign a monotonically increasing sequence number to each packet; and the receiver will detect and store the sequence number. If the receiver gets a packet with an old number, it should discard it and notify to the upper layers the replay attempt.

E. Security Suites

Different forms of the security suites are mentioned as follows:

1) Null: This form of security suite will not offer any security service. It is mandatory to be supported; and all information is sent in the clear.
2) AES-CTR: This form of security suite offers encryption only using the AES cipher in Counter (CTR) mode. In CTR mode, the sender breaks the clear text packet into 16-byte (128 bits).
3) AES-CBC-MAC: This form of security suite offers authentication only using the AES cipher in CBC-MAC mode. The MIC can be 32, 64 or 128 bits long.
4) AES-CCM: This form of security suite offers authentication using the AES cipher in CBC-MAC mode and confidentiality in CTR mode. The MIC can be 32, 64 or 128 bits long.

F. Keying Models

In the case of symmetric encryption, a key must be shared among the parties that want to communicate. Different keying schemes supported by IEEE 802.15.4 are mentioned as follows:

1) Network shared keying: A single key is shared among the network and each station uses that key to communicate with any other station.
2) Pairwise keying: Each pair of nodes shares a unique key, so if a node is compromised, then only that node’s communications are affected. Other communications remain secure.
3) Group keying: This model is a compromise between network shared keying and pairwise keying.

➢ Security Services of UWB

UWB uses the advanced encryption standard (AES) block cipher with counter mode (CTR) and cipher block chaining message authentication code (CBC-MAC) which is also known as CTR with CBC-MAC (CCM), with 32-bit. [30]
Chapter 5

5 Analysis

Wireless communication technology can potentially have a great impact on the weight, size; and cost reduction of the vehicle. This technology also offers the facilities to place the sensing elements in some restricted areas unreachable by wires. Every application for the in-vehicle communication is required certain constraints in terms of data rate, latency and energy consumption. Reliability, dependability, flexibility and predictability are the important attributes among the performance attributes which are also crucial to provide better real-time performance in terms of timeliness, bandwidth utilization and communication delay. Therefore, a single wireless standard has not yet been able to cope with all the needs required in the automotive scenario.

Bluetooth (IEEE 802.15.1) operates in the 2.4 GHz ISM band with speeds up to 3 Mbps. Usually the data rate of Bluetooth is up to 1 Mbps while considering energy efficiency. FHSS (which is used by Bluetooth) is also suitable in harsh environments found in automotive applications. It is widely used for GPS (Global Positioning Systems), receivers, music players or to connect cellular phones. Through Bluetooth interfaces, hand-held computers and diagnostic equipment can interface to the car and access services provided by the on-board diagnostic and control systems. Excluding the mentioned facilities, Bluetooth has several emerging possibilities such as remote starting to warm-up the car in the winter or start the air-conditioning in summer, a remote parking garage or home garage door controller; and payment for gas at the pump and toll road payments.

Technology with low transmission rates, ZigBee (IEEE 802.15.4) operates in three ISM bands (868 MHz, 915 MHz, and 2.4 GHz) at three different data rates (20 Kbps, 40 Kbps, and 250 Kbps, respectively). Interconnection of wireless sensors for control and monitoring is supported by ZigBee where monitoring and control applications are related to temperature and humidity.

Wi-Fi (IEEE 802.11b/g) is the high-rate wireless standard. Wi-Fi operates in the 2.4 GHz band with a data rate of about 6 Mbps. UWB (Ultra-wideband) of IEEE 802.15.3a and 60 GHz millimetre wave of IEEE 802.15.3c technologies are the alternate candidate for Wi-Fi. IEEE 802.15.3a operates at 3.1-10.6 GHz band and its data rate is up to 480 Mbps. IEEE 802.15.3c operates at 60 GHz band and its data rate is greater than 1 Gbps. UWB is a young technology and possibly provides robust communications. The applications of UWB require high bandwidth, such as interconnection of multimedia devices. Collision-detection systems and suspension systems that respond to road conditions could be developed by UWB. These applications are the proposals, as no such applications are available to date. According to our literature study, several challenging applications might have the following wireless solutions. The following table 5.1 shows the comparison among the technology such as Bluetooth, UWB, ZigBee and Wi-Fi.
<table>
<thead>
<tr>
<th>Standards</th>
<th>Bluetooth</th>
<th>UWB</th>
<th>ZigBee</th>
<th>Wi-Fi</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE spec.</td>
<td>802.15.1</td>
<td>802.15.3</td>
<td>802.15.4</td>
<td>802.11a/b/g</td>
</tr>
<tr>
<td><strong>In-vehicle Applications</strong></td>
<td>In-vehicle communication and device connectivity i.e. use in voice application, connect and exchange information between mobile phone, etc.</td>
<td>High speed application In-vehicle communication such as interconnection of multimedia devices etc.</td>
<td>In-vehicle communication i.e. smart lighting control, Remote control, Temperature monitoring, tire sensor, etc.</td>
<td>In-vehicle communication i.e. Internet and multimedia application, informatics etc.</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td>Telematics and Body (low data)</td>
<td>Telematics and powertrain (some non-critical application)</td>
<td>Body (low data)</td>
<td>Telematics</td>
</tr>
<tr>
<td><strong>Data Rate</strong></td>
<td>1 Mbps</td>
<td>100 Mbps</td>
<td>250 Kbps</td>
<td>54 Mbps</td>
</tr>
<tr>
<td><strong>Range</strong></td>
<td>10 meters</td>
<td>10 meters</td>
<td>10-100 meters</td>
<td>100 meters</td>
</tr>
<tr>
<td><strong>Energy Consumption</strong></td>
<td>Low</td>
<td>Ultra-Low</td>
<td>Very-Low</td>
<td>High</td>
</tr>
<tr>
<td><strong>Mode (Spreading)</strong></td>
<td>FHSS</td>
<td>DS-UWB</td>
<td>DSSS</td>
<td>DSSS, CCK, OFDM</td>
</tr>
<tr>
<td><strong>Modulation Type</strong></td>
<td>GFSK</td>
<td>BPSK, QPSK</td>
<td>BPSK, O-QPSK</td>
<td>BPSK, QPSK, COFDM, CCK, M-QAM</td>
</tr>
<tr>
<td><strong>Frequency</strong></td>
<td>2.4 GHz</td>
<td>3.1-10.6 GHz</td>
<td>868 MHz, 915 MHz, 2.4 GHz</td>
<td>2.4 GHz, 5 GHz</td>
</tr>
<tr>
<td><strong>Number of RF Channels</strong></td>
<td>79</td>
<td>(1-15)</td>
<td>1, 10, or 16</td>
<td>14 (2.4 GHz)</td>
</tr>
<tr>
<td><strong>Data Protection</strong></td>
<td>16-bit CRC</td>
<td>32-bit CRC</td>
<td>16-bit CRC</td>
<td>32-bit CRC</td>
</tr>
<tr>
<td><strong>Topology</strong></td>
<td>Star</td>
<td>Peer-to-Peer</td>
<td>Star or Mesh</td>
<td>Star</td>
</tr>
<tr>
<td><strong>Basic Cell</strong></td>
<td>Piconet</td>
<td>Piconet</td>
<td>Star</td>
<td>BSS</td>
</tr>
<tr>
<td><strong>Extension of the Basic Cell</strong></td>
<td>Scatternet</td>
<td>Peer-to-peer</td>
<td>Cluster tree, Mesh</td>
<td>ESS</td>
</tr>
<tr>
<td><strong>Max Number of Cell Nodes</strong></td>
<td>8</td>
<td>8</td>
<td>&gt;65000</td>
<td>Unlimited 2007 (infra-structured)</td>
</tr>
<tr>
<td><strong>Channel Bandwidth</strong></td>
<td>1 MHz</td>
<td>500 MHz-7.5 GHz</td>
<td>0.3, 0.6 MHz; 2 MHz</td>
<td>22 MHz</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>Shared secret</td>
<td>CBC-MAC (CCM)</td>
<td>CBC-MAC (ext. of CCM)</td>
<td>WPA2 (802.11i)</td>
</tr>
</tbody>
</table>

Table 5.1 Comparison of different wireless technologies [29] [30]
In above Table-5.1 represents a side-by-side scenario of the described wireless standards used for in-vehicle applications and focusing particularly on range, data rate, frequency, modulation technique, energy consumption, data protection, topology, basic cell, bandwidth and authentication. The table has shown the example of in-vehicle applications of IEEE 802.15.1, IEEE 802.15.3, IEEE 802.15.4 and IEEE 802.11 with their respective domains and requirements. It is also shown that body domain applications are supported by ZigBee, telematics domains are mostly supported by Bluetooth and Wi-Fi as well as UWB. In case of energy consumption for in-vehicle applications, ZigBee and UWB are the least and Wi-Fi is the most energy consumed technologies. ZigBee and WiFi are much richer in number of supported nodes for Ad hoc operational modes. It is also to be noted that Wi-Fi is the only one to operate in infrastructured operational mode.

Of them, Wi-Fi is dominating over LAN applications and especially used for internet and multimedia applications. ZigBee is suitable for energy efficient, controlling and monitoring in-vehicle applications where as Bluetooth is dominating over PAN applications and suitable for voice application, device connectivity and other in-vehicle applications.

TPMS is a typical wireless application in the field of in-vehicle communication. As we discussed in Chapter 2 section 2.5.2 there are two types of TPMS which could be considered, such as direct TPMS and indirect TPMS. Both of the TPMS, Direct TPMS (based on the pressure sensor installed in each tire) and indirect TPMS (based on the wheel speed and comparing the differences of the tires’ speed) give information or data to the central monitoring system.

As the sensors would be installed in the tire and those are battery-powered, the requirements for this application should be small in size, low energy consumption, and low cost. In this connection, replacing sensor batteries while changing tires is unrealistic and therefore, the sensor batteries are needed to prolong their service life by at least four or five years. The data communication with the central monitoring system is supposed to be of few bits in aspect of the status of measured tire pressure. This communication may happen several times per hour (approximately 6-60 times in an hour) under non-alarm conditions where latency is not a major factor unless quick loss of pressure or an unexpected incident happened for the tire. In the case of an unexpected incident, the central monitoring system should be informed immediately; in such a case energy consumption is not of concern since most likely the tire has to be replaced.

Considering the above-mentioned facts of TPMS, it should be noted that TPMS needs a wireless technology which meets the requirements of very low energy consumption, low data rate and non-criticality. As we can see from the table 4.5, ZigBee is good candidates for TPMS. ZigBee supports such applications for two to five years with two AA batteries.
Bluetooth and Wi-Fi are out of consideration because of their higher energy consumption and worthless high data rate. [32][34]

The automotive temperature varies from section to section of the vehicles and it usually defines 125°C as the high-temperature which is at the engine section. Some temperature sensors such as DS18B20 digital thermometer can be used for temperature monitoring systems inside the vehicle where ZigBee would be a smart solution for such applications. [33]

At present, two wireless standards (such as Bluetooth and Wi-Fi) are practically used in modern cars and these standards are mainly used for multimedia and infotainment applications.

The following table 5.1 expresses the possible in-vehicle applications by the technologies (ZigBee, Bluetooth and WiFi) with their respective bandwidth, frequency and advantages.

From a real-time point of view, none of the wireless technologies presently provide hard real-time guarantees. Wireless technologies are not as deterministic as wired technologies and security issues are also an important concern for the wireless technologies. Existing wired application, such as brake-by-wire or advanced safety and collision avoidance is the example of hard real-time guaranteed application. Therefore real-time dependability concepts are needed for the wireless technologies to provide as good service as possible in the area of wireless real-time communication for in-vehicle applications. [8][6]

From the above discussion and analysis table 2.1, 3.2 and 4.5 we could recommend that the wireless technologies (wireless sensor) mentioned in the following figures can take the place of the wire technologies in-vehicle communication.

Figure 5.1 gives a pictorial presentation of different classes’ placement according to their respective domains and data rate. Figure 5.2 gives a graphical presentation for the positions of ZigBee, Bluetooth and Wi-Fi according to their energy versus data rate measurement, where Wi-Fi takes the highest peak point and ZigBee the lowest.
After having a look at the above figure 5.1 and figure 5.2, we could refer that most of the body applications could be replaced by ZigBee, the applications of powertrain and chassis domain could be partially replaced by Bluetooth. Most of the applications of Telematics could be replaced by Bluetooth, Wi-Fi and UWB.

In summary, among the several wireless technologies ZigBee and Bluetooth are much more preferable while considering low data rate in-vehicle applications with limited energy source, as their low energy consumption leads to a long life-time. In reverse, high data rate in-vehicle applications would be benefited by using UWB and Wi-Fi, because of their low normalized energy consumption.
Chapter 6

6 Conclusion

Through this thesis, the wireless communication for the in-vehicle applications has been analysed. This thesis has presented a broad overview of the four most important wireless standards, IEEE 802.15.1, IEEE 802.15.3, IEEE 802.15.4, and IEEE 802.11 with a literature review in terms of the transmission time, data coding efficiency, protocol complexity, and energy consumption as well as the network size and security. ZigBee and Bluetooth are suitable for low data rate and low energy consumed (which leads to a long life duration) in-vehicle applications. Therefore, this thesis considers ZigBee for the monitoring and control applications as well as TPMS. UWB and Wi-Fi is suitable for high data rate in-vehicle applications. Considered wireless technologies of the thesis are not better candidates for hard real-time applications. It should be borne in mind that the suitability of wireless technologies or protocols for the in-vehicle applications is greatly influenced by practical applications, where factors such as network reliability, recovery mechanism, chipset price and installation cost are needed to be considered carefully.
Acknowledgments

We take pleasure in thanking supervisor for her supervision. Special thanks go to our examiner and gratitude for his benevolent guidelines; and especially for providing very useful and timely suggestions. Without his insight, resources and information, it would have been very difficult to write this thesis.

There are not enough words for our family members. It is really hard to express our gratitude level to them for their immense support. Nevertheless, the support of our friends is always the source of inspiration to move forward.

Finally, we would like to thank the people who have always been present, including our friends and the rest of the Master Thesis students.
References


[23] Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE Std 802.15.4™-2003, Published by: The Institute of Electrical and Electronics Engineers, Inc. 3 Park Avenue, New York, NY 10016-5997, USA, 1 October 2003, Print: SH95127


[26] Part 15.3: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPANs), Published by The Institute of Electrical and Electronics Engineers, Inc 3, Park Avenue, New York, NY 10016-5997, USA 29 September 2003, ISBN 0-7381-3704-9 SH95136
[27] G. Klaus et al. “Choosing the best wireless protocol for typical applications”, Institute of Computer Technology, Vienna University of Technology, Gubhausstrabe 27-29, 1040 Vienna, Austria

[28] Z. Sven, “Coexistence Measurements and Analysis of IEEE 802.15.4 with Wi-Fi and Bluetooth for Vehicle Networks”, 2012 12th International Conference on ITS Telecommunication


[31] T. Jan Magne, “Comparison of the IEEE 802.11, 802.15.1, 802.15.4 and 802.15.6 wireless standards”, September 18, 2007


[34] Li Benliang et al., “The Research of Applying Wireless Sensor Networks to Intelligent Transportation System (ITS) Based on IEEE 802.15.4”, 6th International Conference on ITS Telecommunication Proceedings, 2006


Presentation of Authors

Md Ansrul Haque
Master Student in Information Technology, Halmstad University, Sweden.
Bachelors in Computer Science, SUST, Sylhet, Bangladesh.
Area of Interest: Wireless Communication, Fuzzy Logic and Modern Communication.

Md Delwar Hossain
Master Student in Embedded and Intelligent System, Halmstad University, Sweden.
Bachelors in Computer Science and Engineering, Stamford University Bangladesh, Dhaka, Bangladesh