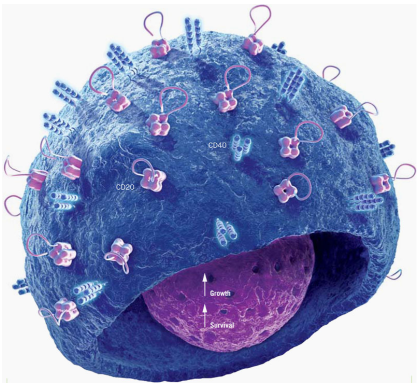

BLE supported indoor location

Subtitle

Ricardo Pacheco Pais Martins

Thesis to obtain the Master of Science Degree in

Elecrical and Computer Engineering

Supervisor(s): Prof./Dr. Lorem Ipsum

Examinatiom Committee

Chairperson: Prof. Lorem
Supervisor: Prof. Lorem Ipsum
Co-Supervisor: Prof. Lorem Ipsum
Members of the Committe: Dr. Lorem Ipsum
Prof. Lorem Ipsum

March 2017

Anyone who has never made a mistake has never tried anything new.

Albert Einstein

Acknowledgments

I would like to thank the Academy,laura, jnos, pais, pais da laura, leal , almeida etc... bla bla bla..

Abstract

The Objective of this Work ... (English)

Keywords

Keywords (English)

Resumo

O objectivo deste trabalho ... (Português)

Palavras Chave

Palavras-Chave (Português)

Contents

List of Figures

List of Tables

Abbreviations

acro acronym

BLE Bluetooth Low Energy

LE Low Energy

IoT Internet of Things

SMP Security Manager Protocol

PHY Physical

QoS Quality of Service

L2CAP Logical Link Control and Adaptation Protocol

HCI Host Controller Interface

P2P Peer-to-Peer

ATT Attribute Protocol The Attribute Protocol

GATT Generic Attribute

GAP Generic Access Profile

FDMA Frequency Division Multiple Access

TDMA Time Division Multiple Access

List of Symbols

1 Introduction

Contents

1.1 Motivation

Motivation Section.

1.2 State of The Art

State of The Art Section.

1.2.1 Dummy Subsection A

State of Art Subsection A

1.2.2 Dummy Subsection B

State of Art Subsection B

1.3 Original Contributions

Contributions Section.

1.4 Thesis Outline

Outline Section.

2

A Chapter

Contents

Present the chapter content.

2.1 Bluetooth Low Energy

Bluetooth is a wireless technology that was created in 1994 with the objective of replacing cables connecting fixed or portable devices. At this point in time Bluetooth Special Interest Group is in charge of developing and managing this technology characterized by its robustness, low energy consuption and low cost.

The Bluetooth Low Energy (BLE) protocol was introduced with the Bluetooth Core Specification version 4 (also called Bluetooth Smart) circa 2010 alongside two other protocols. Out of the three, BLE standed out for its lower power consuption, lower complexity and lower cost, while allowing for device discovery, connection establishment and connection mechanisms. Due to its characteristics, the BLE protocol was utilized in various Internet of Things (IoT) applications.

2.1.1 BLE's Architecture

Bluetooth's Architecture is everchanging and can become very complex rather quickly with the introduction of different types of protocols. When working with BLE it's important to understand the key components of its architecture because by doing it's possible to better analyze the role of each component and how they operate and depend on each other. There are two main groups of core blocks, the Low Energy (LE) Controller and the LE Host, in 2.1.1.A and 2.1.1.B respectively, and most the most relevant of these components will now be looked at.

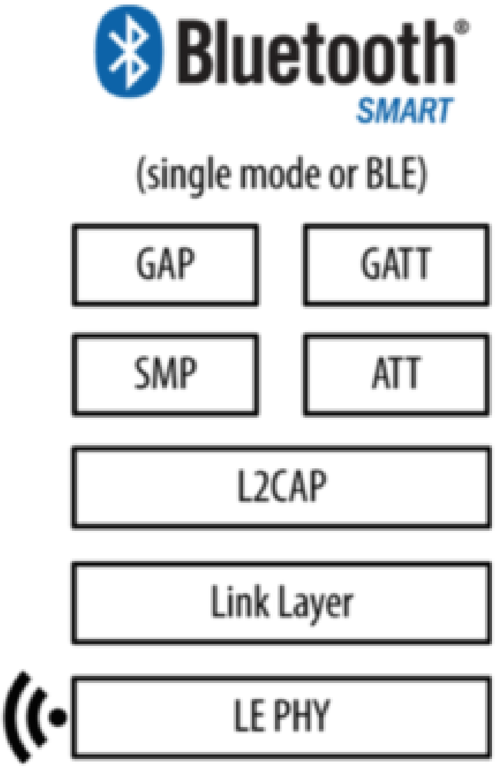

Figure 2.1: BLE architecture

2.1.1.A LE Controller Group

Physical (PHY) Layer - Architectural block responsible for all Bluetooths' communication channels on the 2,4GHz radio. Receiving and transmitting packets and supplying information crucial for controlling its timing and frequency through the baseband block.

Link Layer - Architectural block responsible for managing logical links between BLE devices. It can create and release connections, update connection parameters related to PHY links. It's responsible for the discovery and consequently connection procedure and also sending and receiving data.

Device Manager - Architectural block responsible for controlling the general behaviour of the Bluetooth device. This block is responsible for all operations that aren't directly related to data transportation. Some of its operations are: inquiring for the presence of nearby BLE devices; connecting to a BLE device; setting whether or not its local device is discoverable and/or connectable by the others; controlling device behaviour such as managing own's local name or stored keys.

Baseband Resource Manager - Architectural block responsible for all acess to the radio medium, this means acess to the PHY channels. It has two porpuses, first to negotiate contracts with the entities that wish to use the medium and second to act as a scheduler on the same radio medium, granting the entities with said contracts, a time window in which they can utilize the medium. A contract is basically a commitment to deliver a certain Quality of Service (QoS) on the user application.

Link Controller - Architectural block responsible for the encoding and decoding of Bluetooth packets from the data payload and parameters related to the physical channel, logical transport and logical link. It also carries out the Link Layer protocol in conjunction with Baseband manager's scheduling function to communicate flow control and acknowledgement and retransmission request signals.

2.1.1.B LE Host Group

Logical Link Control and Adaptation Protocol (L2CAP) - Architectural block responsible of transmits packets to the Host Controller Interface (HCI) or directly to the Link Layer in hostless systems. It allows for higher-level protocol multiplexing, packet segmentation and reassembly, and the conveying of QoS information to higher layers.

Channel Manager - Architectural block responsible for creating, managing and closing L2CAP channels used in transport of service protocols and application data streams. The local Channel Manager makes use of the L2CAP protocol to communicate with a peer's Channel Manager and together create L2CAP channels and connect their endpoints to the appropriate entities.

Security Manager Protocol (SMP) - Architectural block responsible for implementing the Peer-to-Peer (P2P) protocol that operates over its own dedicated L2CAP channel and generates encryption keys and identity keys. This block is also in charge of storing those same keys and making them available to the controller. These keys are later used in the encryption or pairing procedures.

Generic Access Profile (GAP) - Architectural block responsible for working in conjunction with Generic Attribute (GATT) to define the base funcionality of BLE devices. The available services in this profile are: BLE device discovery, connection modes, security, authentication, association models and service discovery. GAP defines four different roles to describe a device, allowing for the controllers to be optimized in funtion of the device's desired roles. **Broadcaster:** This role is optimized for transmitter-only applications. In a scenario in which a device supports this role it will make use of advertising in order to broadcast its data. The broadcaster role doesn't support for connections.

Observer: This role is optimized for receiver-only applications and it's complementary to the broadcaster role. It only receives broadcast data included in advertising packets and much like its counterpart, it doesn't support connections.

Peripheral: This role is optimized for devices that only want to suppot a single connection, allowing for a much less complex controller due to the fact that it only needs to support the slave role and not the master one.

Central: This role supports multiple connections and funtions as the initiator for all of them. These connection are all made with Peripheral devices and its controller must support the master role in a connection and allow for more complex funtions, in comparison to the remaining roles.

Attribute Protocol The Attribute Protocol (ATT) Protocol - Architectural block responsible for implementing the P2P protocol between an attribute server and client. This client/server communication happens in a dedicated fixed L2CAP channel. A server can send through this channel responses, notifications and indications, while the client can send requests, commands and confirmations. This block allows the clients to read and write values of attributes on a peer device acting as a ATT server.

GATT Profile - Architectural block responsible for creating a framework for the ATT, in which it is represented the funcionalities of an ATT server. This profile describes the hierarchy of services, characteristics and attributes existent in the server and provides an interface for discovering, reading, writing and indicating of service characteristics and profiles. A more thorough description of profiles can be found in 2.1.2. GATT also defines two possible roles, which aren't directly tied to the GAP roles previously presented but can be specified by higher layer profiles. **Server:** A GATT server is responsible for storing data transported over the ATT and accepts ATT requests, commands and confirmations from a GATT client. It also sends responses to requests and, if implemented, send indication and notification asynchronously to a GATT client when specified events occur on the GATT server.

Client: A GATT client has all the functionalities presented in the GATT server description.

2.1.2 BLE Profiles

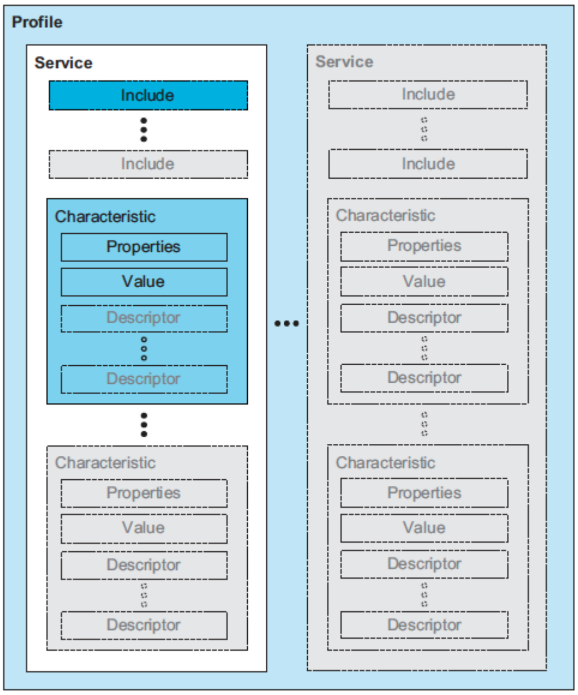

Figure 2.2: Gatt-based profile hierarchy

Bluetooth profiles defines the required functionalities of each layer, from the PHY to the L2CAP layer, aswell as the the vertical interactions between layers and P2P interactions between device and a specific layer. Since a profile also defines application behaviour and data formats, we can say that when two devices comply with all the requirements of a Bluetooth profile, application interoperability is achieved. Each Bluetooth profiles describes its requirements necessary for devices to create a connection, to find available services and connection information required for making application level connections.

The base profile that any Bluetooth system needs to include is the GAP, already presented in 2.1.1.B. From this point, any additional profile implemented will be a superset of GAP, where GATT is included. Among all that was already introduced about GATT in 2.1.1.B, it also specifies the profile hierarchy, or the structure in which profile data is exchanged. 2.2 shows the hierarchy in a Gatt-based profile, with the profile being the top level and services and characteristics below. The last two will now be presented individualy:

Service: A profile is composed by one or more services. CITAÇÂO CORE PAGE 256 A service is a collection of data and associated behaviors to accomplish a particular function or feature of a device or portions of a device. It can be either primary, which provides primary funcionalities of a device, or secundary, providing auxiliary functionalities of a device and is referenced from at least one primary service. A service is composed of characteristics and/or references to other services.

Characteristic: A Characteristic is a value that is used in a service that has properties and configuration information that descrive how the value should be accessed as well as information on how to display the value. A characteristic is defined by its declaration, its properties, its value and may also be defined by its descriptor, which describes the value or permit configuration of the server relative to the value.

2.1.3 Communication Topology and Operation

The LE radio operates at the 2.4GHz band and employs a frequency hopping transceiver to combat interference and fading. LE also employs two multiple access schemes: Frequency Division Multiple Access (FDMA) used to separate the 40 available PHY channels, 37 of them are used as data channels and the remaining as advertising channels and Time Division Multiple Access (TDMA) in a polling scheme that is used when one device transmits a packet at a predetermined time and a corresponding device responds with a packet after a predetermined interval.

The PHY channels are sub-divided into time units known as events and these can be of two types according to which type of channel they belong, either advertising events or data events.

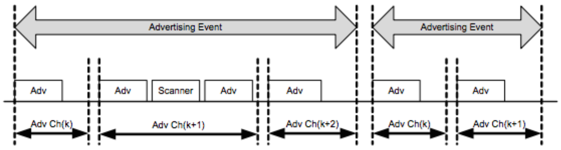

Figure 2.3: Advertising event

Advertising events: There are three roles that can be used to describe a device in function of their utilization of the channel: **advertisers**, are those that transmit advertising packets; **scanners** are devices that receive advertising packets without the intention of connecting with the advertising device; **initiators** are devices that listen for connectable advertising packets in order to later initiate a connection. Transmissions in the advertising channels occur in advertising events which always start with an advertiser sending a packet. Depending on the type of advertising packet, a scanner device may make a request to the advertiser which may be followed by a response from the advertiser, always on the same advertising PHY channel. The advertising PHY channel changes when the advertiser sends a new advertising packet. An advertising event can be terminated whenever the advertiser wants and when a new advertising event is created it will occur in the first advertising PHY channel. The whole process can be visualized in 2.3.

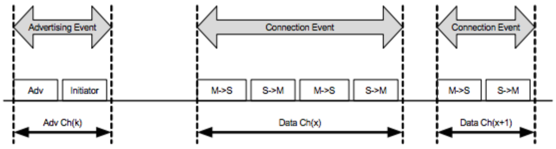

Figure 2.4: Connection event

Connection events: When an advertiser is using a connectable advertising event an initiator may request a connection on the same PHY channel. If the advertiser accepts the connection request, the advertising event ends and a connection event starts in order to establish the connection. Once it's established the initiator takes the master role and the advertised, the slave role. These events are used to transmit data between eachother and they always begin with a message from the master. During a connection event master and slave alternate send data packets on the same packet. The master is responsible for ending the end whenever he pleases and for the creation of new event channel hopping is required. The whole connection event can be visualized in 2.4.

2.1.3.A LE Piconet Topology

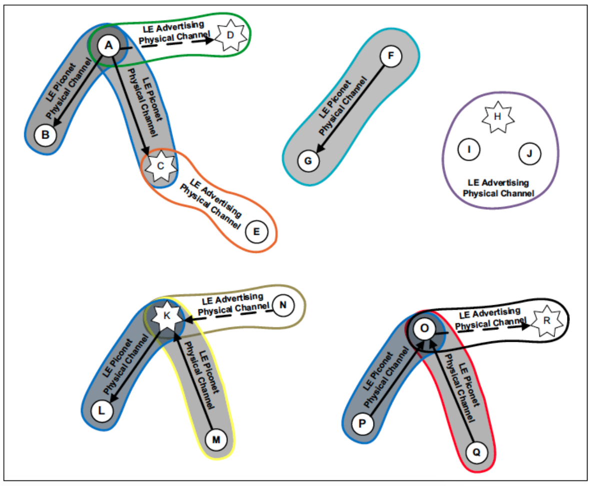
A
LE Advertising Physical Channel
D
LE Piconet Physical Channel
B
LE Piconet Physical Channel
C
LE Advertising Physical Channel
E
F
LE Piconet Physical Channel
G
H
I
J
LE Advertising Physical Channel
K
LE Advertising Physical Channel
N
LE Piconet Physical Channel
L
LE Piconet Physical Channel
M
O
LE Advertising Physical Channel
R
LE Piconet Physical Channel
P
LE Piconet Physical Channel
Q

Figure 2.5: Examples of LE topology

In Figure 4.2 an example topology is shown that demonstrates a number of the LE architectural features described below. Device A is a master in a piconet (represented by the shaded area, and known as piconet A) with devices B and C as slaves. Unlike BR/EDR slaves, LE slaves do not share a common physical channel with the master. Each slave communicates on a separate physical channel with the master. One other piconet is shown with device F as master (known as piconet F) and device G as a slave. Device K is in a scatternet (known as scatternet K). Device K is master of device L and slave of device M. Device O is also in a scatternet (known as scatternet O). Device O is slave of device P and slave of device Q. Note: in the figure, solid arrows point from master to slave; dashed arrows, indicating a connection initiation, point from initiator to advertiser using a connectable advertising event; devices that are advertising are indicated using stars. There are five other groups of devices shown: 1. Device D is an advertiser and device A is also an initiator (known as group D). 2. Device E is a scanner and device C is also an advertiser (known as group C). 3. Device H is an advertiser and devices I and J are scanners (known as group H). 4. Device K is also an advertiser and device N is an initiator (known as group K). 5. Device R is an advertiser and device O is also an initiator (known as group R). Devices A and B are using one LE piconet physical channel (represented by the blue enclosure and a dark gray background). Devices A and C are using another LE piconet physical channel (represented by the blue enclosure and a lighter gray background). In group D, device D is advertising using a connectable advertising event on the advertising physical channel (represented by the green enclosure) and device A is an initiator. Device A can form a connection with device D and add the device to piconet A. In group C, device C is also advertising on the advertising physical channel (represented by the orange enclosure) using any type of advertising events that are being captured by device E as a scanner. Group D and group C may be using different advertising PHY channels or different timings to avoid collisions. In piconet F, there is one physical channel. Devices F and G are using an LE piconet physical channel (represented by the aqua enclosure). Device F is the master and device G is the slave. In group H, there is one physical channel. Devices H, I and J are using an LE advertising physical channel (represented by the purple enclosure). Device H is an advertiser and devices I and J are scanners. In scatternet K, devices K and L are using one LE piconet physical channel. Devices K and M are using another LE piconet physical channel. In group K, device K is also advertising using a connectable advertising event on the advertising physical channel and device N is an initiator. Device N can form a connection with device K resulting in device K being slave of two devices and master of one device at the same time. In scatternet O, devices O and P are using one LE piconet physical channel. Devices O and Q are using another LE piconet physical channel. In group R, device R is advertising using a connectable advertising event on the advertising physical channel and device O is an initiator. Device O can form a connection with device R resulting in device O being slave of two devices and master of one device at the same time.

2.1.3.B Operational Procedure

The typical operational mode of a Bluetooth device is to be connected to other Bluetooth devices (in a piconet) and exchanging data with those Bluetooth devices. As Bluetooth is an ad-hoc wireless communications technology, there are a number of operational procedures that enable piconets to be formed so that the subsequent communications can take place. Procedures and modes are applied at different layers in the architecture and therefore a device may be engaged in a number of these procedures and modes concurrently.

4.2.2.1 Device Filtering Procedure The device filtering procedure is a method for controllers to reduce the number of devices requiring communication responses. Since it is not required to respond to requests from every device, it reduces the number of transmissions an LE Controller is required to make which reduces power consumption. It also reduces the communication the controller would be required to make with the host. This results in additional power savings since the Host does not have to be involved. An advertising or scanning device may employ device filtering to restrict the devices from which it receives advertising packets, scan requests or connection requests. In LE, some advertising packets received by a scanning device require that the scanning device send a request to the advertising device. This advertisement can be ignored if device filtering is used and the advertising device is being filtered. A similar situation occurs with connection requests. Connection requests must be responded to by advertisers unless a device filter is used to limit the devices to which the advertiser is required to respond. Advertisers can also use device filters to limit the devices in which it will accept a scan request or connection request. This device filtering is accomplished through the use of a “White List” located in the LL block of the controller. A white list enumerates the remote devices that are allowed to communicate with the local device. When a white list is in effect, transmissions from devices that are not in the white list will be ignored by the LL. Since device filtering occurs in the LL it can have a significant impact on power consumption by filtering (or ignoring) advertising packets, scan requests or connection requests from being sent to the higher layers for handling. The use of device filtering during certain procedures needs to be evaluated carefully to ensure devices are not unintentionally ignored, which may cause interoperability problems when attempting to establish connections or receive advertising broadcasts.

4.2.2.2 Advertising Procedure An advertiser uses the advertising procedure to perform unidirectional broadcasts to devices in the area. The unidirectional broadcast occurs without a connection between the advertising device and the listening devices. The advertising procedure can be used to establish connections with nearby initiating devices or used to provide periodic broadcast of user data to scanning devices listening on the advertising channel. The advertising procedure uses the advertising physical channel for all advertising broadcasts. An LE device connected in an LE piconet may advertise using any type of advertising event. Time spent advertising while connected needs to be balanced with the connection requirements needed to maintain the already established connection(s) (if the device is a slave in the piconet then it needs to maintain its connection with the master and if the device is the master it needs to maintain its connection(s) with the one or more slaves in the piconet). Advertising devices may receive scan requests from listening devices in order to get additional user data from the advertising device. Scan responses are sent by the advertising device to the device making the scan request over the same advertising physical channel. Whereas the broadcast user data sent as part of the advertising packets is typically dynamic in nature, scan response data is generally static in nature. An advertising device may receive connection requests from initiator devices on the advertising broadcast physical channel. If the advertising device was using a connectable advertising event and the initiating device is not being filtered by the device filtering procedure, the advertising device ceasesadvertising and enters the connected mode. The device can begin advertising again after it is in the connected mode.

4.2.2.3 Scanning Procedure A scanning device uses the scanning procedure to listen for unidirectional broadcasts of user data from advertising devices using the advertising physical channel. A scanning device can request additional user data from an advertising device by making a scan request over the advertising physical channel. The advertising device responds to these requests with additional user data sent to the scanning device over the advertising physical channel. The scanning procedure can be used while connected to other LE devices in an LE piconet. Time spent scanning while connected needs to be balanced with the connection requirements needed to maintain the already established connection with the other LE devices in the piconet. If the broadcasts are connectable advertising events and the scanning device is in the initiator mode, it can initiate a connection by sending a connection request on the advertising broadcast physical channel to the advertising device. Once the connection request is sent, the scanning device ceases the initiator mode scanning for additional broadcasts and enters the connected mode. The device can use the scanning procedure after it enters the connected mode. For a master device, using the initiator mode and scanning for connectable advertisements is how additional devices can be added to the master's LE piconet.

4.2.2.4 Discovering Procedure Bluetooth devices use the advertising procedure and scanning procedure to discover nearby devices, or to be discovered by devices in a given area. The discovery procedure is asymmetrical. A Bluetooth device that tries to find other nearby devices is known as a discovering device and listens for devices advertising scannable advertising events. Bluetooth devices that are available to be found are known as discoverable devices and actively broadcast scannable advertising events over the advertising broadcast physical channel. Both discovering and discoverable devices may already be connected to other Bluetooth devices in a piconet. Any time spent inquiring or occupying the advertising broadcast physical channel needs to be balanced with the connection requirements needed to maintain the already established connection with the other LE devices in the piconet. Using device filtering by the scanning device will prevent the scanning device from discovering all the devices in a given area.

4.2.2.5 Connecting Procedure The procedure for forming connections is asymmetrical and requires that one Bluetooth device carries out the advertising procedure while the other Bluetooth device carries out the scanning procedure. The advertising procedure can be targeted, so that only one device will respond to the advertising. The scanning device can also target an advertising device by first discovering that the advertising device is present in a connectable manner, and in the given area, and then scanning only connectable advertising events from that device using the device filter. After receiving connectable advertising events from the targeted advertising device, it can initiate a connection by sending the connection request to the targeted advertising device over the advertising broadcast physical channel. Time spent scanning while connected needs to be balanced with the connection requirements needed to maintain the already established connection with the other LE devices in the piconet.

4.2.2.6 Connected Mode After a successful connection procedure, the devices are physically connected to each other within a piconet. This means that there is a piconet physical channel to which they are both connected, there is a physical link between the devices, and there are default LE-C and LE-U logical links. When in the connected mode it is possible to change the properties of the physical and logical links while remaining connected to the piconet physical channel, such as changing the adaptive frequency hopping sequence or changing the length of data packets. It is also possible for the device to carry out advertising, scanning or discovery procedures without needing to disconnect from the original piconet physical channel. Additional logical links are created using the Link Manager that exchanges LL Protocol messages with the remote Bluetooth device to negotiate the creation and settings for these links. One of these links (LE-C) transports the LL control protocol and is invisible to the layers above the Link Manager. The other link (LE-U) transports the L2CAP signaling protocol and any multiplexed L2CAP best-effort channels. It is common to refer to a default LE ACL logical transport, which can be resolved by context, but typically refers to the default LE-U logical link. Also note that these two logical links share a logical transport. During the time that a slave device is actively connected to a piconet there is always a default LE ACL logical transport between the slave and the master device. The method of deleting the default LE ACL logical transport is to detach the device from the piconet physical channel, at which time the entire hierarchy of L2CAP channels, logical links, and logical transports between the devices is deleted.

acronym (acro)

acronym (acro)

acro

acronym

acros

As seen in [1]. *Enfatizar*

Remember you can change the reference style. Another dummy citation [2].

2.2 Section B

2.2.1 Subsection A

The model described can also be represented as

$$\dot{\mathbf{x}}(t) = \mathbf{T}\mathbf{z}(y),\ \mathbf{y}(0) = \mathbf{y}_0,\ z \geq 0 \tag{2.1}$$

where

$$\mathbf{A} = \left[\begin{array}{cc} -(a_{12}+a_{10}) & a_{21} \\ a_{12} & -(a_{21}+a_{20}) \end{array} \right],\ \mathbf{x} = \left[\begin{array}{c} x_1 \\ x_2 \end{array} \right] \tag{2.2}$$

2.2.2 Subsection B

Table 2.1: Dummy Table.

Vendor Name	**Short Name**	**Commercial Name**	**Manufacturer**
Text in Multiple Row	ABC	ABC®	ABC SA
	DEF	DEF®	DEF SA
	GHF	GHF®	GHF SA
Text in Single Row	IJK	IJK®	IJK SA
Frescos SA	LMN	LMN®	LMN SA
Carros Lda.	Text in Multiple Column		

3

Conclusions and Future Work

Bibliography

[1] “Wikipedia,” http://www.wikipedia.org, 2011.

[2] R. Dummy, “How to write a Latex Article,” http://www.biopsychiatry.com/misc/genetic-defects.html, August 2011.

A

Title of AppendixA