WAVE: A Tutorial

Roberto A. Uzcátegui

Guillermo Acosta-Marum

Presenter – Renato Iida

Outline

- Introduction

- WAVE SYSTEM ARCHITECTURE

- PHY and MAC Layers

- Multichannel Operation

- Networking Services

- Resource Manager

- Security Services

- Concluding Remarks

Worcester Polytechnic Institute

Introduction

Motivation and Standards

Motivation

- Intelligent Vehicle Highway Systems (IVHS) US,1991
  - Increase safety
  - Ameliorate congestion
  - Reduce pollution
  - Conserve fossil fuel

- DOT advices with Intelligent Transportation Society of America (ITSA)

- Created the intelligent transportation system [ITS] in 1996
  - http://www.its.dot.gov/

Worcester Polytechnic Institute

Standard of WAVE

- 2004, IEEE create the network layers based on ITSA

- 802.11p describe the PHY/MAC layer
  - Based on 802.11a
  - Uses 5.85-5.925 GHz
  - 75 Mhz of spectrum

- 1609 describe the other layer
  - Divided in 4 parts

- Wireless Access in Vehicular Environments (WAVE) is the solution using both standards

WAVE: A Tutorial

Worcester Polytechnic Institute

# WAVE SYSTEM ARCHITECTURE

Types and elements

Types of Networks

- Vehicle-to-Vehicle(V2V)
  - Connect between two or Onboard units (OBUs)

- Vehicle-to-Infrastructure(V2I)
  - Connect between Onboard units (OBUs) and Roadside units (RSUs)

- Traditional Internet Access

Worcester Polytechnic Institute

Organization and Channels

- Exchange information using control channel (CCH) and operates independently

- WAVE basic service sets
  - Small Network
  - Similar to 802.11 service set
  - Mix of OBU and RSU
  - Service channels (SCHs)

WAVE: A Tutorial

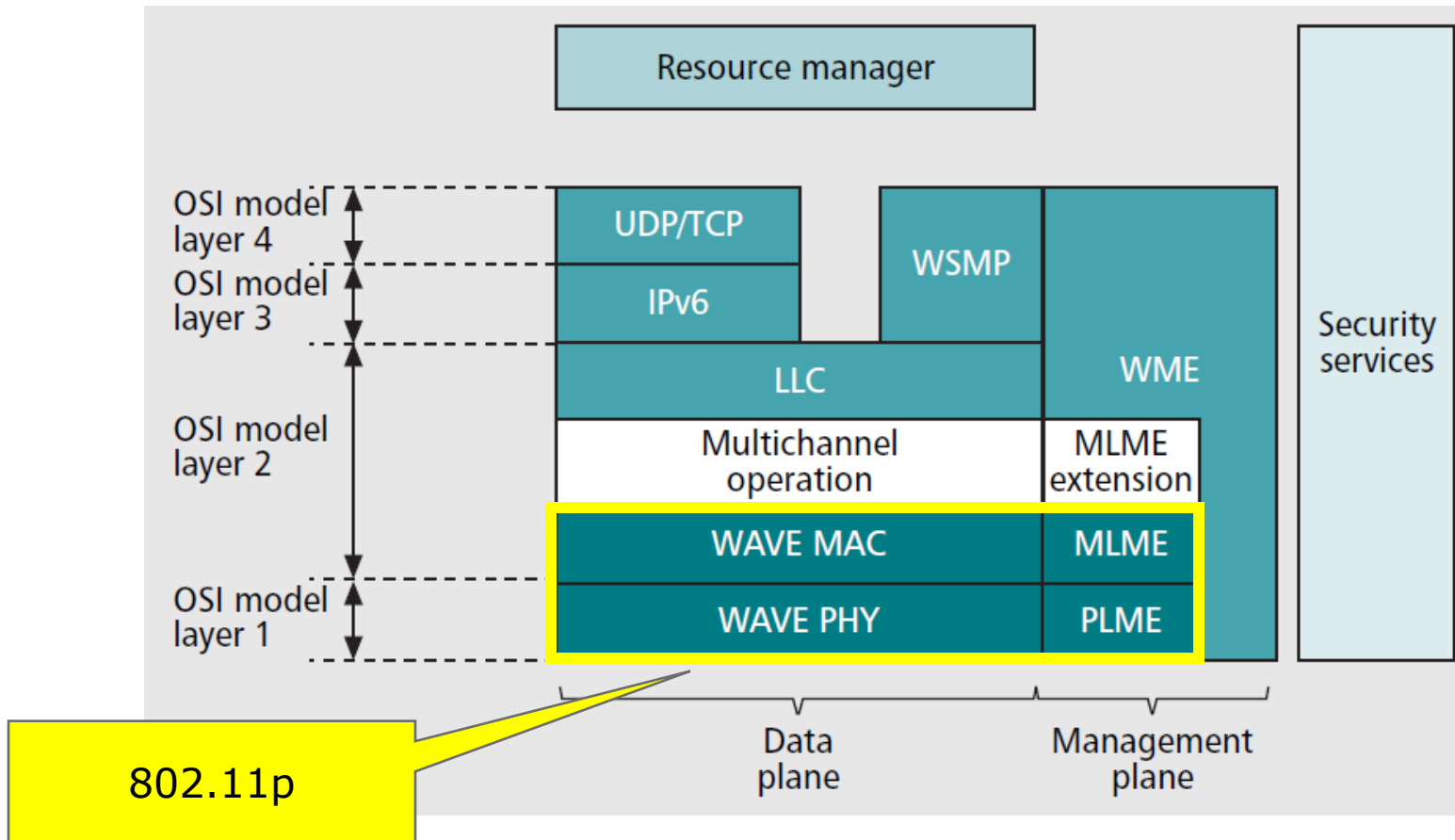Worcester Polytechnic Institute

Examples
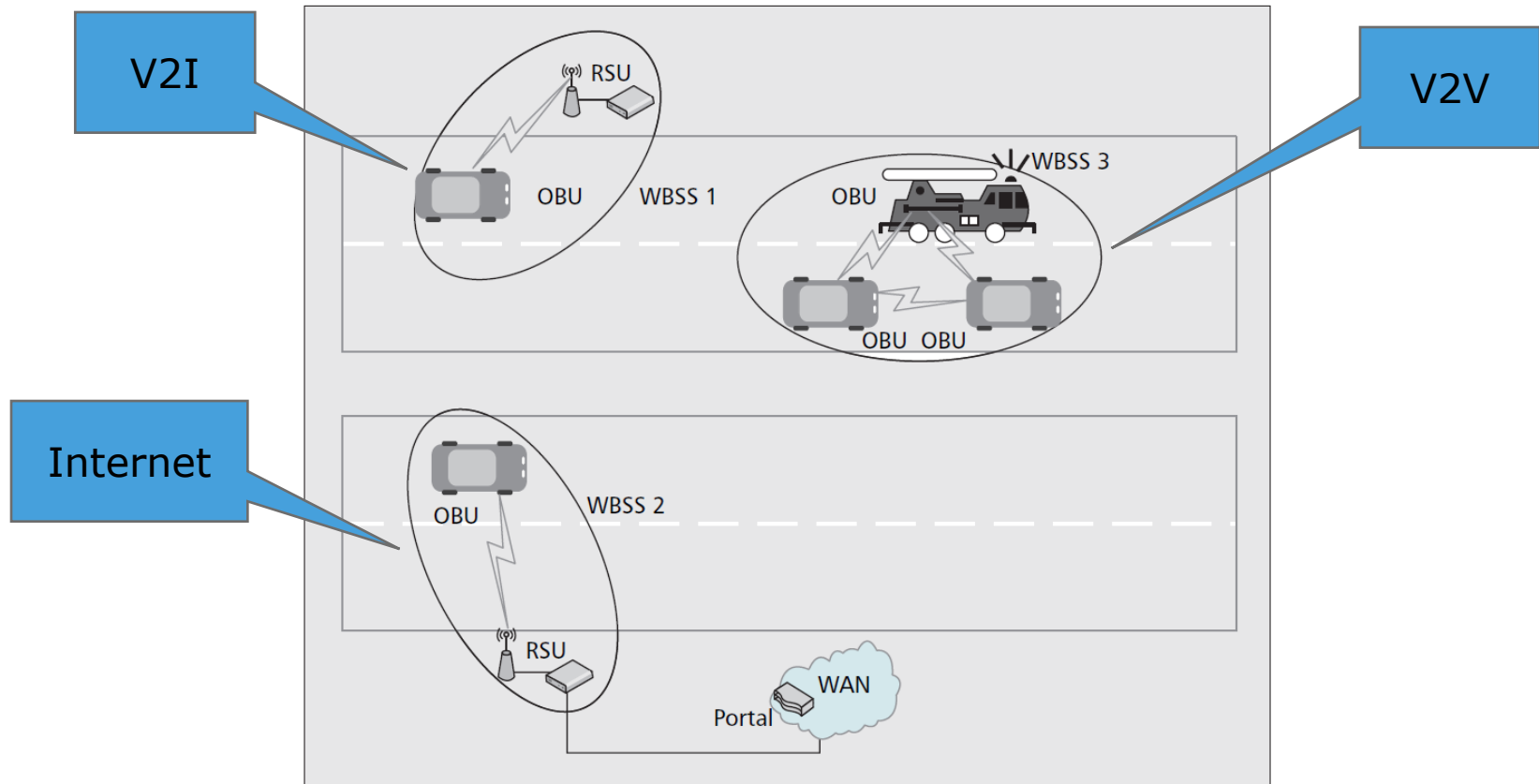
Figure 1. *Illustration of a WAVE system showing the typical locations of the OBUs and RSUs, the general makeup of the WBSSs, and the way a WBSS can connect to a WAN through a portal.*

Worcester Polytechnic Institute

PHY and MAC layers

802.11p

WAVE: A Tutorial

Protocol Stack

WAVE: A Tutorial

Worcester Polytechnic Institute

Requirement

- Longer ranges of operations (up to 1000m)
- The high speed of vehicles
- Extreme multipath environments
- Multiple overlapping ad hoc with QoS
- Special beacon frame

Worcester Polytechnic Institute
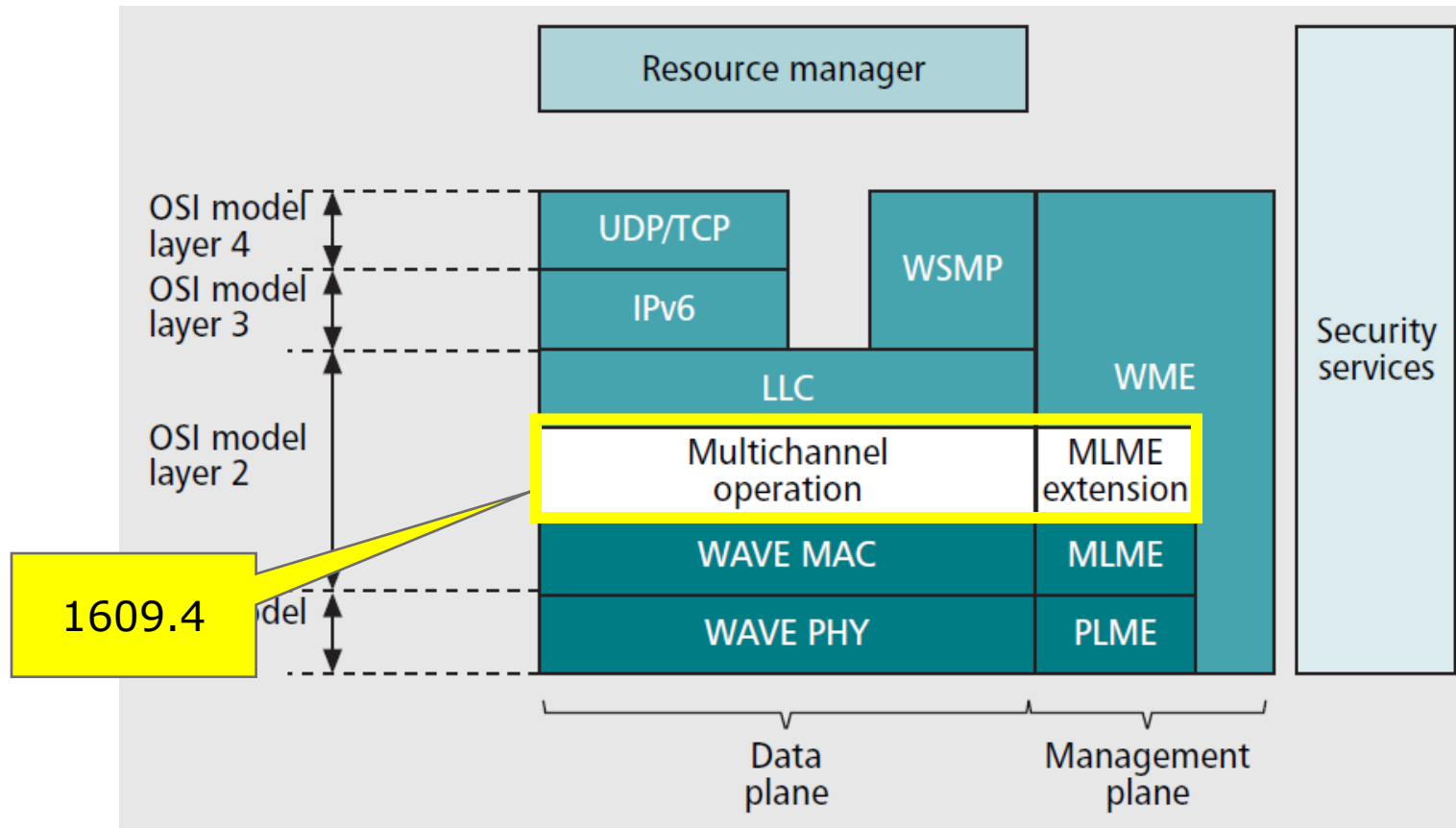
Implementation

- 10 Mhz channels , half of the 802.11a

- Control Channel and six service channel

- Unique ad hoc mode

- Random MAC

- High accuracy of RSSI

- 16 QAM lower rate than 802.11a

- Priority control

- Power Control

Worcester Polytechnic Institute

Multichannel Operation

Functional Description

Protocol Stack

Worcester Polytechnic Institute

Elements of Multichannel Operation

- Medium access using enhanced distributed channel access (EDCA) from 802.11e

- Enhancement to IEEE 802.11 MAC

- Manage channel coordination and to support MAC service data unit (MSDU)

Worcester Polytechnic Institute

Services

- Control channel data transfer
- Service channel data transfer
- Data transfer services
- Control priority of data packet (WSMP or IP)
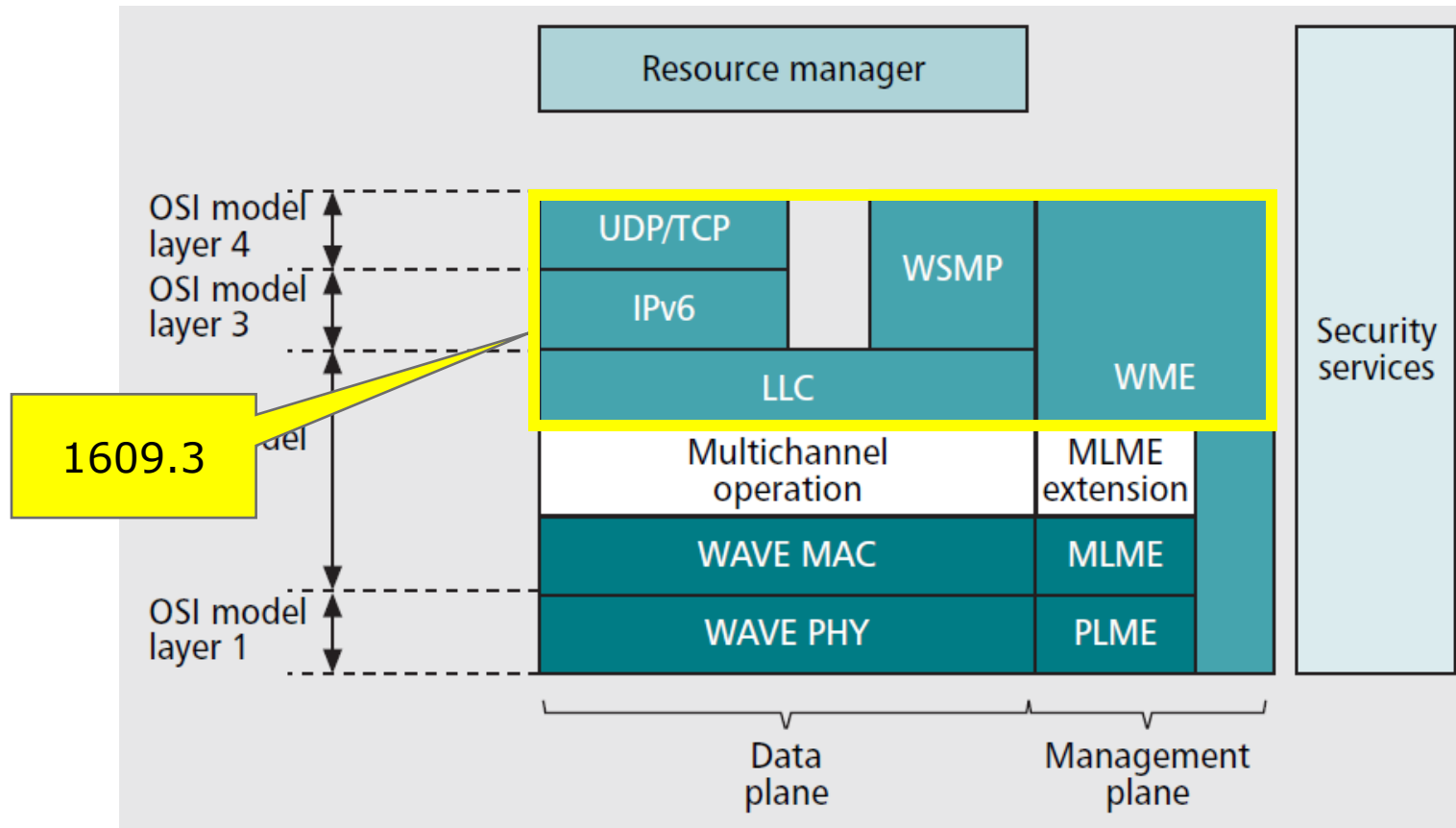
Worcester Polytechnic Institute

Functional Description

- Management Frames
  - Wave announcement only in CCH
  - Other IEEE management frames

- Data Frames
  - Wave short message can be on CCH and SCH
  - IP data frames only on SCH

- Channel Coordination using CCH
  - For each WBSS

Worcester Polytechnic Institute

Network Services

WAVE: A Tutorial

Protocol Stack

WAVE: A Tutorial

Worcester Polytechnic Institute

Data Plane Services

- IPv6
  - TCP
  - UDP

- WSMP
  - Capable of forward message
  - Check integrity of the message

Worcester Polytechnic Institute

Management-Plane Services

- Application registration

- WBSS management

- Channel usage monitoring

- IPv6 configuration

- Received channel power indicator (RCPI) monitoring

- Management information base (MIB) maintenance

Worcester Polytechnic Institute

Application Registration

- All applications need to register with WAVE management entity [WME]

- Each application registers with a unique provider service identifier (PSID)

- Three tables
  - ProviderServiceInfo – info about applications that provide service
  - UserServiceInfo -applications residing in the local unit
  - ApplicationStatus – Info about the applications

Worcester Polytechnic Institute

WBSS Management

- Link establishment

- Addition or removal of applications from dynamic WBSSs

- Inclusion (provider side) and retrieval (user side) of security credentials

- WBSS termination

- Maintenance of the status of each application in the context of a particular WBSS

Worcester Polytechnic Institute

Channel Usage Monitoring

- Mandate that WME tracks SCH usage

- The standard don't define how but need to choose a less congested channel

Worcester Polytechnic Institute

IPv6 Configuration

- Controls the IPv6 connections

Worcester Polytechnic Institute

RCPI Monitoring

- Any application can query a remote device about the strength of the received signal

- MLME that handle this request

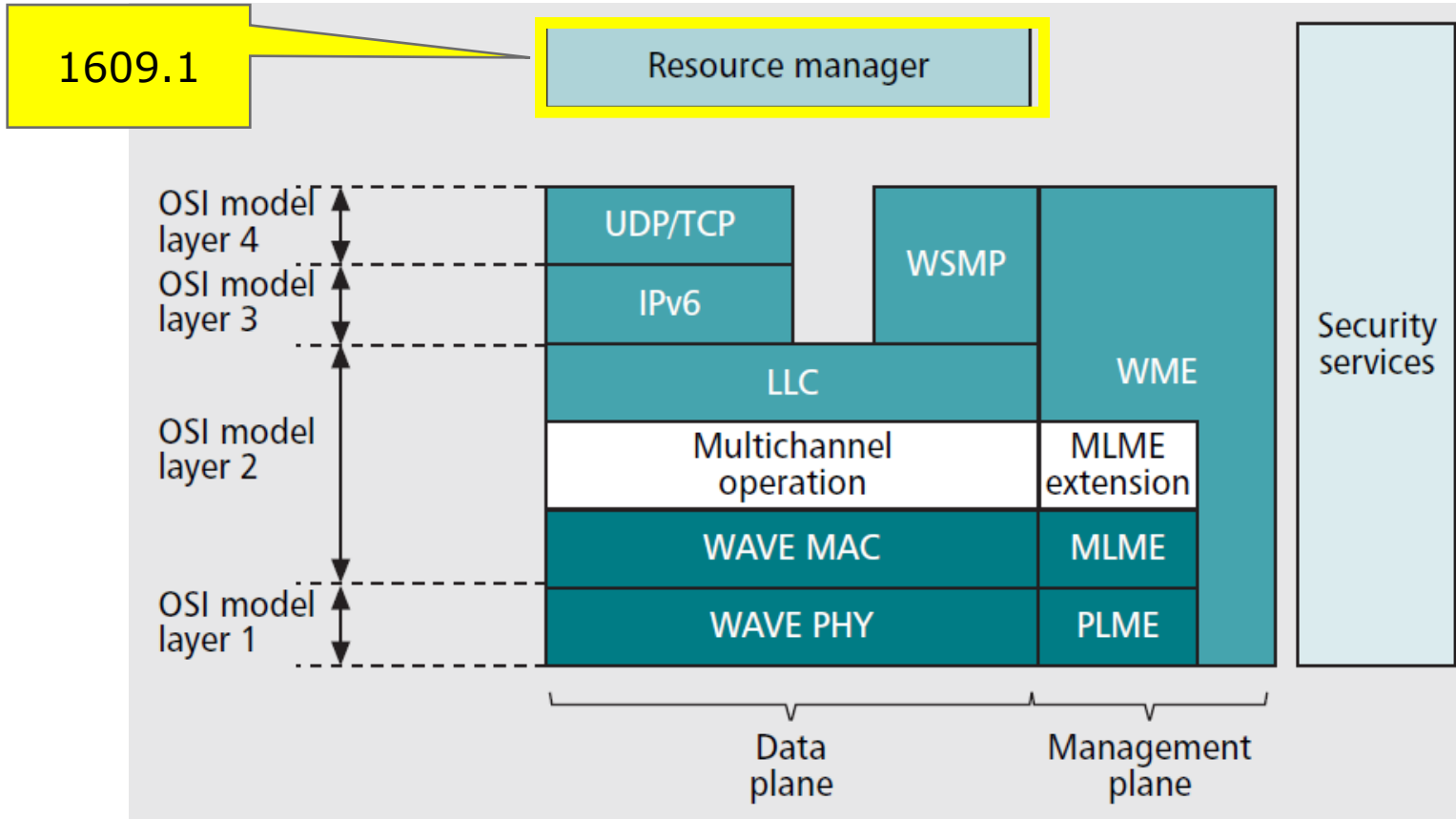WAVE: A Tutorial

Worcester Polytechnic Institute

MIB Maintenance

- The WME maintains a MIB that contains system-related and application-related information

- Examples
  - Network Information
  - Addresses information
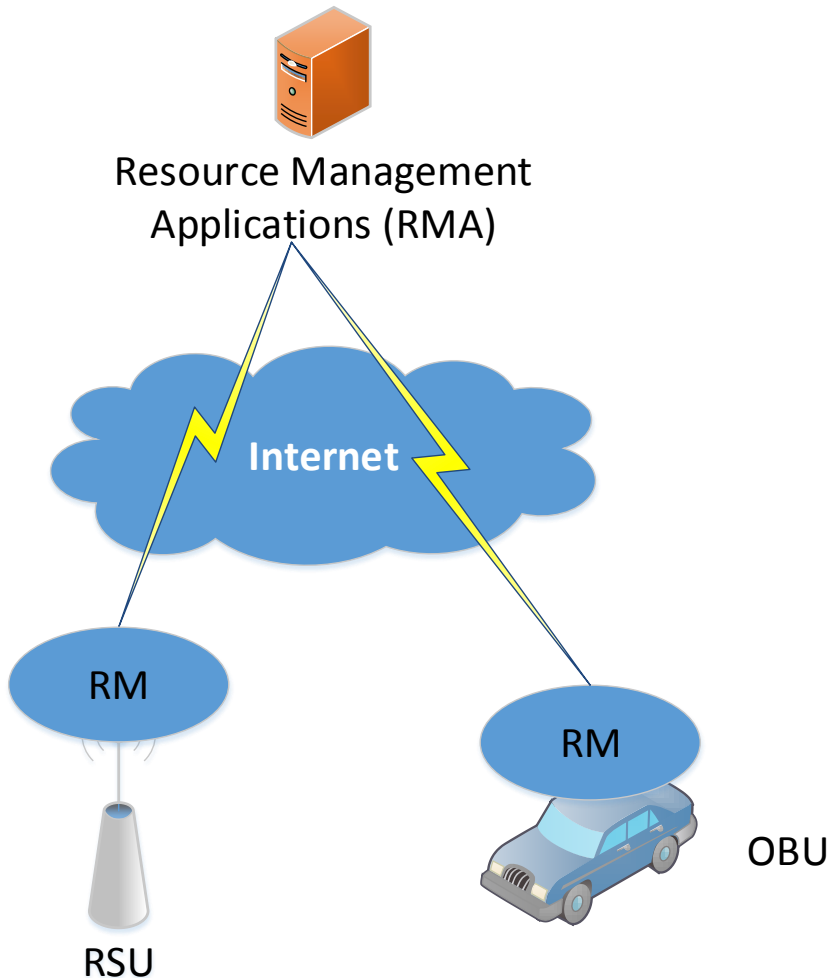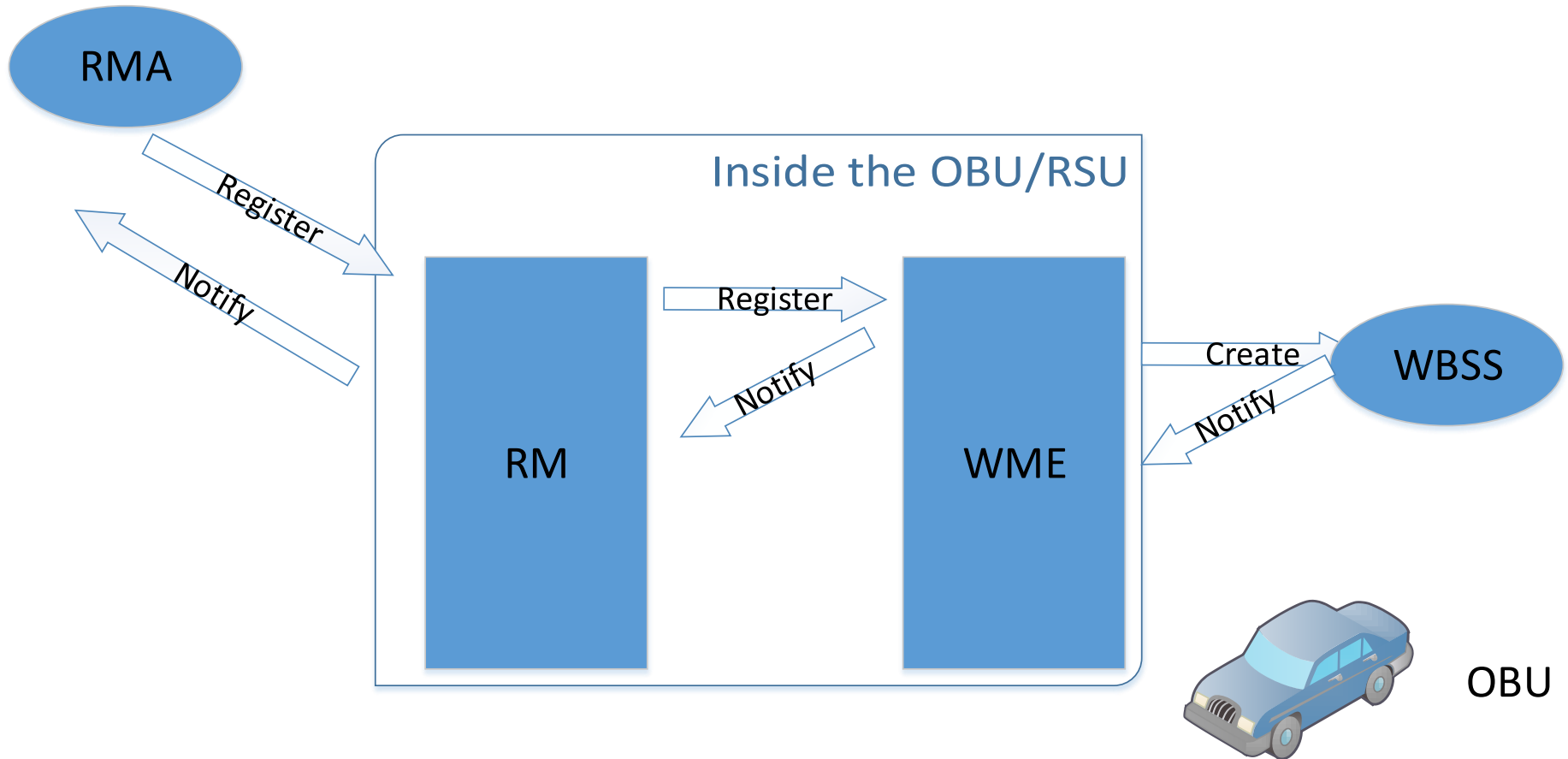 - Registration port
  - And others

Worcester Polytechnic Institute

Resource Manager

WAVE: A Tutorial

Protocol Stack

WAVE: A Tutorial

Worcester Polytechnic Institute

Elements in the network

Resource Management
Applications (RMA)

Internet

RM

RM

RSU

OBU

- RM have a resource command processor (RCP)

- RPC executes the command inside the RM on behalf of RMA

Worcester Polytechnic Institute

Inside the OBU/RSU

WAVE: A Tutorial

Worcester Polytechnic Institute

Security Services

WAVE: A Tutorial

Protocol Stack

WAVE: A Tutorial

Worcester Polytechnic Institute
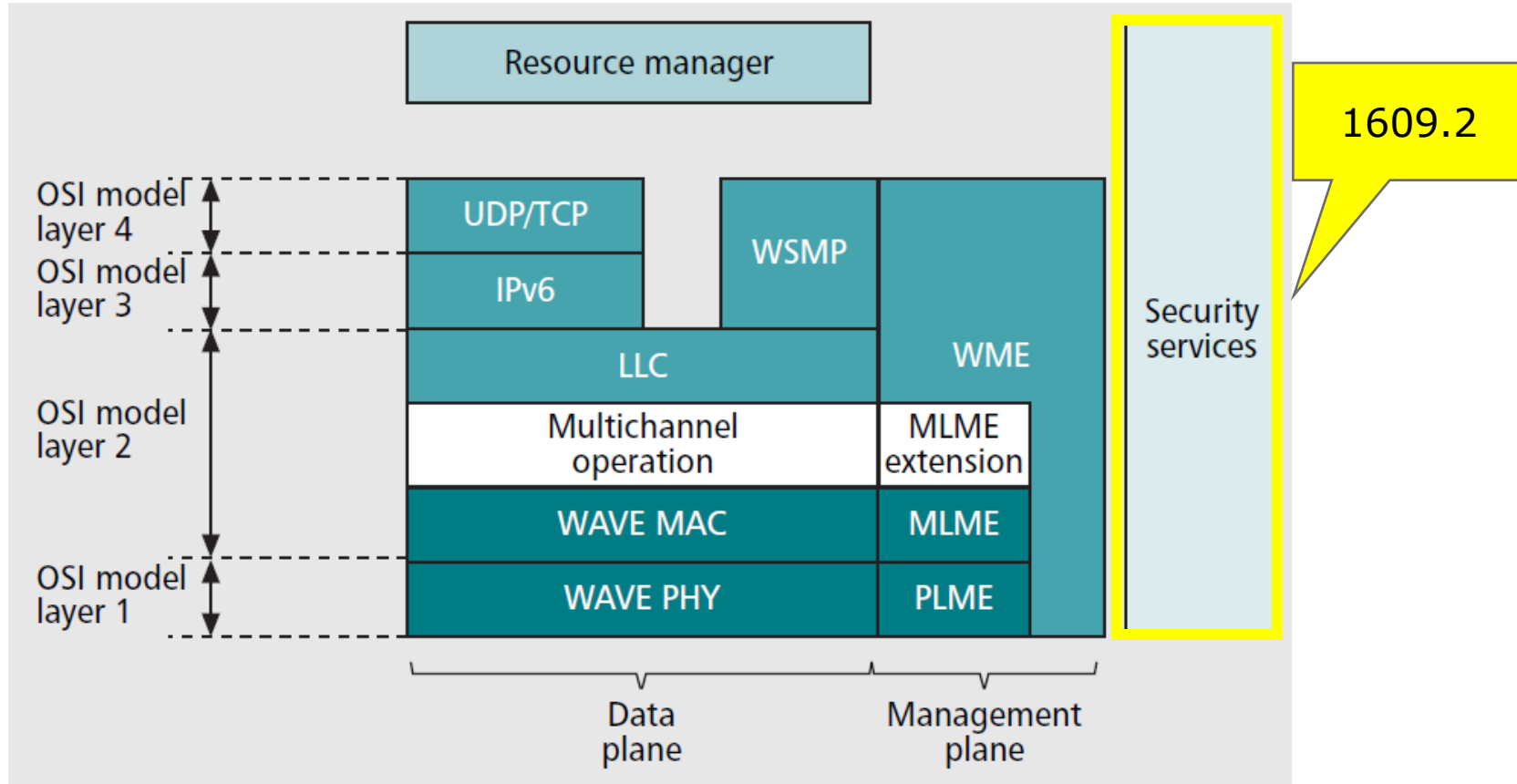
Symmetric Algorithms

- How it can be used
  - Encrypted-only
  - Authenticated-only
  - Both

- Use Message Integrity Check (MIC)

- Algorithm CBC AES-CCM

Worcester Polytechnic Institute

Remaining Algorithms

- Support Asymmetric Keys

- User SHA1 for hash functions

- Don't guarantee anonymous header in the broadcast messages

Worcester Polytechnic Institute

Hash Function

- Use to create the MIC

- Uses SHA-1

Conclusions

- Show how WAVE fit in a OSI model

- Based on well-known solution of 802.11

- Test of ITS were on going in California,Michigan, New York and Virginia

Worcester Polytechnic Institute

Extra

- https://www.udacity.com/course/applied-cryptography--cs387

Worcester Polytechnic Institute