ANALYSIS OF COMMUNICATION PROTOCOLS FOR HOME AREA NETWORKS
FOR SMART GRID

Mayur Anand
B.E, Visveswaraiah Technological University, Karnataka, India, 2007

PROJECT

Submitted in partial satisfaction of
the requirements for the degree of

MASTER OF SCIENCE

in

COMPUTER SCIENCE

at

CALIFORNIA STATE UNIVERSITY, SACRAMENTO

SPRING
2011
ANALYSIS OF COMMUNICATION PROTOCOLS FOR HOME AREA NETWORKS FOR SMART GRID

A Project

by

Mayur Anand

Approved by:

__________________________________, Committee Chair
Isaac Ghansah, Ph.D.

__________________________________, Second Reader
Chung-E-Wang, Ph.D.

__________________________________
Date
Student: Mayur Anand

I certify that this student has met the requirements for format contained in the University format manual, and that this project is suitable for shelving in the Library and credit is to be awarded for the Project.

__________________________, Graduate Coordinator       ________________
Nikrouz Faroughi, Ph.D.                             Date
Department of Computer Science
Abstract

of

ANALYSIS OF COMMUNICATION PROTOCOLS FOR HOME AREA NETWORKS
FOR SMART GRID

by

Mayur Anand

This project discusses home area networks in Smart Grid. A Home Area Network plays a very important role in communication among various devices in a home. There are multiple technologies that are in contention to be used to implement home area networks. This project analyses various communication protocols in Home Area Networks and their corresponding underlying standards in detail. The protocols and standards covered in this project are ZigBee, Z-Wave, IEEE 802.15.4 and IEEE 802.11. Only wireless protocols have been discussed and evaluated. Various security threats present in the protocols mentioned above along with the counter measures to most of the threats have been discussed as well. Some of the threats where the counter measures are inadequate have been identified as potential areas of research.
DEDICATION

This project is dedicated to my parents H.M Anand, Poornima Anand, my brother Vachan Anand and my sister-in-law Pooja Vachan.
ACKNOWLEDGMENTS

It is a pleasure to thank everyone who helped me in successfully completing my Masters’ Project.

First and foremost I would like to thank my project supervisor, Dr. Isaac Ghansah, Professor, Computer Science and Engineering for giving me an opportunity to work under his guidance, and for providing me constant support throughout the project. My heartfelt thanks to Dr.Chung-E Wang for agreeing to be my second reader and providing me with his invaluable feedback on revising my report.

I am also very grateful to Dr. Nikrouz Faroughi, Graduate Coordinator, Department of Computer Science and Engineering, for his invaluable feedback and suggestions.

I would like to thank my friends Pooja Ramesh and Vinod Thirumurthy who helped me in reviewing this report.

Finally yet importantly, I would like to thank my parents, H.M.Anand and Poornima Anand, and my brother Vachan Anand for their moral and financial support. I am very grateful for their continuous support and never ending encouragement that they have provided throughout my life. They have always motivated me and are the sole reason for me to have come this far in life.
TABLE OF CONTENTS

Dedication…………………………………………………………………………………………….v
Acknowledgements………………………………………………………………………………vi
List of Tables…………………………………………………………………………………….xiii
List of Figures……………………………………………………………………………………xiv
List of Abbreviations……………………………………………………………………………..xvii

Chapter

1. INTRODUCTION………………………………………………………………………………1
   1.1 The Traditional Grid……………………………………………………………………1
   1.2 Need for Smart Grid……………………………………………………………………3
   1.3 Smart Grid………………………………………………………………………………7
   1.4 Literature Review……………………………………………………………………11
   1.5 Scope of the Project……………………………………………………………………12

2. HOME AREA NETWORKS…………………………………………………………………14
   2.1 What is a Home Area Network………………………………………………………14
   2.2 Role of Home Area Networks in Smart Grid………………………………………14

3. UNDERLYING MAC PROTOCOLS AND STANDARDS………………………………20
   3.1 IEEE 802.15.4……………………………………………………………………………20
      3.1.1 Introduction to IEEE 802.15.4……………………………………………………20
      3.1.2 IEEE 802.15.4 Architecture……………………………………………………23
      3.1.2.1 PHY……………………………………………………………………………24
3.1.2.2 MAC Layer……………………………………………………………………….26
3.1.2.2.3 Superframe Structure………………………………………………………….28
3.1.2.3 Data Transfer Model……………………………………………………………….30
3.1.2.3.1 Data Transfer to a Coordinator………………………………………………31
3.1.2.3.2 Data Transfer from a Coordinator…………………………………………32
3.1.2.3.3 Peer-to-Peer Data Transfer………………………………………………….34
3.1.2.4 Frame Structure…………………………………………………………………….35
3.1.2.4.1 Beacon Frame…………………………………………………………………35
3.1.2.4.2 Data Frame……………………………………………………………………36
3.1.2.4.3 Acknowledgment Frame……………………………………………………38
3.1.2.4.4 MAC Command Frame…………………………………………………….39
3.1.2.4.4.1 Robustness…………………………………………………………………39
3.1.2.4.4.1.2 CSMA-CA Mechanism………………………………………………40
3.1.2.4.4.1.3 Frame Acknowledgment………………………………………………45
3.1.2.4.4.1.4 Data Verification………………………………………………………46
3.1.2.5 Power Consumption Considerations…………………………………………46
3.1.2.6 IEEE 802.15.4 Security Overview……………………………………………47
3.1.2.6.1 AES-CTR Security Suite………………………………………………….51
3.1.2.6.2 AES-CBC-MAC Security Suite…………………………………………….53
3.1.2.6.3 AES-CCM Security Suite………………………………………………….53
3.2 IEEE 802.11…………………………………………………………………………………54
3.2.1 Introduction to IEEE 802.11…………………………………………………………54
3.2.2 IEEE 802.11 Architecture..............................................................57
  3.2.2.1 802.11 Physical Layer.........................................................58
  3.2.2.2 802.11 MAC Layer.............................................................63
    3.2.2.2.1 The Hidden Node Problem............................................64
  3.2.2.3 802.11 Framing.................................................................66
  3.2.2.4 802.11 Security Specification.............................................67

4. COMMUNICATION PROTOCOLS IN HOME AREA NETWORKS.................70
  4.1 Z-Wave........................................................................................70
    4.1.1 Introduction............................................................................70
    4.1.2 Z-Wave Protocol Architecture..............................................71
      4.1.2.1 Controllers.................................................................73
        4.1.2.1.1 Portable Controller.................................................74
        4.1.2.1.2 Static Controller....................................................74
        4.1.2.1.3 Static Update Controller .......................................74
        4.1.2.1.4 SUC ID Server.........................................................75
        4.1.2.1.5 Installer Controller................................................75
        4.1.2.1.6 Bridge Controller....................................................76
      4.1.2.2 Slaves............................................................................76
        4.1.2.2.1 Routing Slave.........................................................77
        4.1.2.2.2 Enhanced Slave.......................................................77
      4.1.2.3 Home ID and Node ID.....................................................77
    4.1.2.4 MAC Layer........................................................................78
4.2.2.1.2 ZigBee Device Objects.................................................................96
4.2.2.1.3 Application Support Sub-Layer (APS)........................................97
  4.2.2.1.3.1 Application Support Sub-Layer Data Entity (APSDE).................97
  4.2.2.1.3.2 Application Support Sub-Layer Management Entity (APSME).....98
4.2.2.2 Network (NWK) Layer Overview..................................................99
  4.2.2.2.1 Network Layer Data Entity (NLDE)..........................................100
  4.2.2.2.2 Network Layer Management Entity (NLME)..............................101
4.2.2.3 ZigBee Security Specification.....................................................102
  4.2.2.3.1 Security Design Choices.......................................................104
  4.2.2.3.2 ZigBee Security Architecture................................................106
    4.2.2.3.2.1 MAC Layer Security......................................................107
    4.2.2.3.2.2 NWK Layer Security....................................................109
    4.2.2.3.2.3 APL Layer Security......................................................110
  4.2.2.3.3 Security Keys Establishment................................................111
  4.2.2.3.4 Trust Center Role...............................................................112

5. SECURITY ISSUES AND VULNERABILITIES.........................................114
  5.1 IEEE 802.15.4 Security Vulnerabilities............................................114
  5.2 IEEE 802.11 Security Vulnerabilities...............................................116
  5.3 Z-Wave Security Vulnerabilities......................................................118
  5.4 ZigBee Security Vulnerabilities......................................................119

6. COUNTER MEASURES AND BEST PRACTICES......................................121
  6.1. 802.15.4 Counter Measures and Best Practices..................................121
LIST OF TABLES

Page

Table 1-1: Comparison of Traditional Grid vs. Smart Grid.................................6

Table 3-1: Security suites supported by 802.15.4.............................................49

Table 3-2: Security services offered by the various security suites supported by IEEE 802.15.4-2003..................................................................................50

Table 3-3: Variants of 802.11 Standard...............................................................56
## LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1-1</td>
<td>The Traditional Grid</td>
<td>2</td>
</tr>
<tr>
<td>Figure 1-2</td>
<td>Smart Grid</td>
<td>8</td>
</tr>
<tr>
<td>Figure 1-3</td>
<td>How Smart Grid works</td>
<td>10</td>
</tr>
<tr>
<td>Figure 2-1</td>
<td>Communication between Utility and Consumer</td>
<td>15</td>
</tr>
<tr>
<td>Figure 2-2</td>
<td>Use of HAN in Smart Grid</td>
<td>17</td>
</tr>
<tr>
<td>Figure 2-3</td>
<td>An example of the role of HAN in demand – response</td>
<td>18</td>
</tr>
<tr>
<td>Figure 3-1</td>
<td>A summary of IEEE 802.15.4 characteristics</td>
<td>22</td>
</tr>
<tr>
<td>Figure 3-2</td>
<td>IEEE 802.15.4 in the context of other related IEEE Standards</td>
<td>23</td>
</tr>
<tr>
<td>Figure 3-3</td>
<td>LR-WPAN device architecture</td>
<td>24</td>
</tr>
<tr>
<td>Figure 3-4</td>
<td>Superframe Structure without guaranteed time slots</td>
<td>28</td>
</tr>
<tr>
<td>Figure 3-5</td>
<td>Superframe structure with guaranteed slots</td>
<td>29</td>
</tr>
<tr>
<td>Figure 3-6</td>
<td>Communication to a coordinator in a beacon-enabled network</td>
<td>31</td>
</tr>
<tr>
<td>Figure 3-7</td>
<td>Communication to a coordinator in a non beacon-enabled network</td>
<td>32</td>
</tr>
<tr>
<td>Figure 3-8</td>
<td>Communication from a coordinator in a beacon-enabled network</td>
<td>33</td>
</tr>
<tr>
<td>Figure 3-9</td>
<td>Communication from a coordinator in a non beacon-enabled network</td>
<td>34</td>
</tr>
<tr>
<td>Figure 3-10</td>
<td>Schematic view of the beacon frame</td>
<td>36</td>
</tr>
<tr>
<td>Figure 3-11</td>
<td>Schematic view of the data frame</td>
<td>37</td>
</tr>
<tr>
<td>Figure 3-12</td>
<td>Schematic view of the acknowledgement frame</td>
<td>38</td>
</tr>
<tr>
<td>Figure 3-13</td>
<td>Schematic view of the MAC command frame</td>
<td>39</td>
</tr>
<tr>
<td>Figure 3-14</td>
<td>CSMA-CA Algorithm</td>
<td>43</td>
</tr>
</tbody>
</table>
Figure 3-15: Format of an ACL entry ......................................................... 48

Figure 3-16: Format of input (Xi) to the block cipher for AES-CTR and AES-CCM modes .......................................................... 52

Figure 3-17: Format of the data field in the AES-CTR Security Suite ......................... 52

Figure 3-18: Format of data field in the AES-CBC-MAC Security suite ..................... 53

Figure 3-19: Format of data field in the AES-CCM Security suite ........................ 54

Figure 3-20: 802.11 in relation to the ISO Model .............................................. 58

Figure 3-21: IEEE 802.11 Physical layer components ........................................ 59

Figure 3-22: Major Components of 802.11 ...................................................... 61

Figure 3-23: ESS Provides Campus-Wide Coverage .......................................... 63

Figure 3-24: Hidden Node Problem .................................................................. 65

Figure 3-25: RTS and CTS address the Hidden Node Problem .......................... 66

Figure 3-26: WEP Shared Key Authentication ................................................. 68

Figure 4-1: Z-Wave Protocol Layers .............................................................. 72

Figure 4-2: A sample Z-Wave Network ........................................................... 73

Figure 4-3: Z-Wave basic frame format ........................................................... 79

Figure 4-4: Singlecast Frame Transfer ............................................................. 80

Figure 4-5: Multicast Frame Transfer ................................................................ 81

Figure 4-6: Broadcast Frame Transfer ............................................................. 82

Figure 4-7: Routed Singlecast and Acknowledgement Frame Type ....................... 84

Figure 4-8: Network topology and routing table ............................................. 85

Figure 4-9: Z-Wave Application Frame Format ............................................... 87
Figure 4-10: Command Classes in Z-Wave.........................................................87
Figure 4-11: Controller requesting Node information........................................89
Figure 4-12: Comparison of Z-Wave and ZigBee.................................................90
Figure 4-13: Outline of the ZigBee Stack Architecture.......................................93
Figure 4-14: The NWK Layer Reference Model...............................................100
Figure 4-15: ZigBee Frame with security at the MAC level...............................108
Figure 4-16: ZigBee Frame with security on the NWK level...............................110
Figure 4-17: ZigBee Frame with security at the frame level...............................110
LIST OF ABBREVIATIONS

ACL      Access Control List
ACL      Access Control List
AES      Analog Encryption Scheme
AES-CBC-MAC Analog Encryption Scheme Cipher Block Chaining Message Authentication Code
AES-CCM  Analog Encryption Scheme Counter with CBC-MAC
AES-CTR  Analog Encryption Scheme Counter Mode
AIB      APS information base
AMI-SEC  Advanced Metering Infrastructure Security
ANSI     American National Standards Institute
AP       Access Point
APDU     Application Level Protocol Data Unit
APDU     Application Protocol Data Unit
APL      Application Layer
APS      Application Support Sub-layer
APSDE    Application Support Sub-Layer Data Entity
APSDE-SAP Application Support Sub-Layer Data Entity Service Access Point
APSME    Application Support Sub-Layer Management Entity
APSME    APS Management Entity
APSME-SAP APSME Service Access Point
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BE</td>
<td>Backoff Exponent</td>
</tr>
<tr>
<td>BP</td>
<td>Backoff Period</td>
</tr>
<tr>
<td>BSN</td>
<td>Beacon Sequence Number</td>
</tr>
<tr>
<td>BSS</td>
<td>Basic Service Set</td>
</tr>
<tr>
<td>CAP</td>
<td>Contention Access Period</td>
</tr>
<tr>
<td>CBC-MAC</td>
<td>Cipher Block Chaining Message Authentication Code</td>
</tr>
<tr>
<td>CCA</td>
<td>Clear Channel Assessment</td>
</tr>
<tr>
<td>CCM</td>
<td>Counter with CBC-MAC mode of operation</td>
</tr>
<tr>
<td>CCM*</td>
<td>Enhanced counter with CBC-MAC mode of operation</td>
</tr>
<tr>
<td>CFP</td>
<td>Contention Free Period</td>
</tr>
<tr>
<td>CRC</td>
<td>Cyclic Redundancy Check</td>
</tr>
<tr>
<td>CSMA-CA</td>
<td>Carrier Sense Multiple Access - Collision Avoidance</td>
</tr>
<tr>
<td>CTS</td>
<td>Clear to Send</td>
</tr>
<tr>
<td>CW</td>
<td>Contention Window</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>DS</td>
<td>Distribution System</td>
</tr>
<tr>
<td>DSM</td>
<td>Demand Side Management</td>
</tr>
<tr>
<td>DSSS</td>
<td>Direct sequence spread spectrum</td>
</tr>
<tr>
<td>ED</td>
<td>Energy Detection</td>
</tr>
<tr>
<td>EEPROM</td>
<td>Electronically Erasable Programmable read only memory</td>
</tr>
</tbody>
</table>
EOF        End Of Frame
ESS        Extended Service Set
FCC        Federal Communications Commission
FCS        Frame Check Sequence
FCS        Frame check sequence
FFD        Fully Functional Device
FHSS       Frequency hopping spread spectrum
FSK        Frequency Shift Keying
GPS        Global Positioning System
GTS        Guaranteed Time Slots
HAN        Home Area Network
IBSS       Independent Basic Service Set
IDS        Intrusion Detection systems
IEC        International Electrotechnical Commission
IEEE       Institute of Electrical and Electronics Engineers
ISO        International Organization for Standardization
ITU-T      International Telecommunication Union - Telecommunication Standardization Sector
IV         Initial Vector
IV         Initialization Vector
LLC        Logical Link Control
LQI        Link Quality Indication
LR-WPAN Low-Rate Wireless Personal Area Networks

MAC Media Access Control

MCPS-SAP Medium Access Control common part sub-layer - service access point

MFR Media Access Control Layer Footer

MHR Media Access Control Layer Header

MIC Message Integrity Code

MLME MAC Management Entity

MLME-SAP Medium Access Control Sub-Layer Management Entity - Service Access Point

MPDU MAC Protocol Data Unit

MRD Marketing Requirements Document

MSDU MAC Service Data Unit

NB Number of Backoff

NIST National Institute of Standards and Technology

NLDE Network Layer Data Entity

NLME NWK layer management entity

NWK Network Layer

OFDM Orthogonal frequency division multiplexing

OpenHAN Open Home Area Network

OSI Open Systems Interconnection

PAN Personal Area Network

PDU Application Protocol Data Unit
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHR</td>
<td>Physical Layer Header</td>
</tr>
<tr>
<td>PHY</td>
<td>Physical Layer</td>
</tr>
<tr>
<td>PIB</td>
<td>Personal Area Network Information Base</td>
</tr>
<tr>
<td>PIR</td>
<td>Passive Infra Red</td>
</tr>
<tr>
<td>PIR</td>
<td>Passive Infra Red Movement Sensor</td>
</tr>
<tr>
<td>PLME</td>
<td>Physical Layer Management Entity</td>
</tr>
<tr>
<td>PPDU</td>
<td>Physical Layer Protocol Data Unit</td>
</tr>
<tr>
<td>PSDU</td>
<td>PHY service data unit</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
</tr>
<tr>
<td>RFD</td>
<td>Reduced Functional Device</td>
</tr>
<tr>
<td>RREQ</td>
<td>Route Request messages</td>
</tr>
<tr>
<td>RTS</td>
<td>Request to Send</td>
</tr>
<tr>
<td>SAP</td>
<td>Service Access Point</td>
</tr>
<tr>
<td>SDO</td>
<td>Standards Development Organizations</td>
</tr>
<tr>
<td>SEP</td>
<td>Smart Energy Profile</td>
</tr>
<tr>
<td>SFD</td>
<td>Start of Frame Delimiter</td>
</tr>
<tr>
<td>SHR</td>
<td>Synchronization Header</td>
</tr>
<tr>
<td>SIS</td>
<td>SUC ID Server</td>
</tr>
<tr>
<td>SKKE</td>
<td>Symmetric-Key Key Establishment</td>
</tr>
<tr>
<td>SRS</td>
<td>Software Requirement Specification</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>SSCS</td>
<td>Service Specific Convergence Sub-Layer</td>
</tr>
<tr>
<td>SSID</td>
<td>Service Set Identifier</td>
</tr>
<tr>
<td>SUC</td>
<td>Static Update Controller</td>
</tr>
<tr>
<td>TKIP</td>
<td>Temporal Key Integrity Protocol</td>
</tr>
<tr>
<td>TRD</td>
<td>Technical Requirements Document</td>
</tr>
<tr>
<td>UCAIug</td>
<td>UCA International User’s Group</td>
</tr>
<tr>
<td>UPnP</td>
<td>Universal Plug and Play</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>WEP</td>
<td>Wired Equivalent Privacy</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>Wireless Fidelity</td>
</tr>
<tr>
<td>WPA</td>
<td>Wi-Fi Protected Access</td>
</tr>
<tr>
<td>WPAN</td>
<td>Wireless Personal Area Networks</td>
</tr>
<tr>
<td>ZDO</td>
<td>Zigbee Device Objects</td>
</tr>
</tbody>
</table>
Chapter 1

INTRODUCTION

1.1 The Traditional Grid

The traditional grid or the power grid is the largest interconnected machine on Earth and is over a century old. It is so complex and human involved that it has alternately been called an ecosystem. It consists of more than 9,200 electric generating units with more than 1,000,000 megawatts of generating capacity connected to more than 300,000 miles of transmission lines [1]. The National Academy of Engineering compiled an estimable list of twenty accomplishments which have affected virtually everyone in the developed world. On this list, the internet took thirteenth place. At the top of the list is electrification made possible by the power grid.

The Figure 1-1 [2] shows the traditional power grid right from the generation of electricity at the power plants. The three-phase power leaves the generator and enters a transmission substation at the power plant which uses large transformers to convert the generator's voltage to higher appropriate voltages for long-distance transmission on the transmission grid. The high transmission lines transmit to a power sub station where the voltage is stepped down before transmitting over the medium voltage power lines to the customer premises. The pole-top transformer drums further step down the voltage to suit the residential and commercial specifications.
The traditional power grid as shown above is a producer controlled model where electricity flows from the producer to the consumer. The grid needs to be able to handle to accept power from as well as provide power to consumers. In many areas of the United States, the only way a utility knows there’s an outage is when a customer calls to report it. This is the sort of communication between the grid and the consumers that is required but is missing in the traditional grid. The current grid also does not have the capability for supplying consumers with demand response information in real time so that consumers can make an informed decision to use less energy at peak time.
Since 1982, growth in peak demand for electricity – driven by population growth, bigger houses, bigger TVs, more air conditioners and more computers – has exceeded transmission growth by almost 25% every year [1]. Throughout the United States, only 668 additional miles of interstate transmission have been built since 2000, even as demand has skyrocketed. Yet spending on research and development is among the lowest of all industries [1]. As a result, the grid has begun to fail more frequently and presents substantial risks. Also, concerns such as energy efficiency and customer choice were of marginal importance at the time the traditional grid was formed. Energy efficiency is of much higher importance now due to ever increasing power demand. In short, the traditional grid is struggling to keep up.

1.2 Need for Smart Grid

Various shortcomings of the traditional grid were discussed in the previous section. The following are reasons for a smarter grid:

Reliability: There have been quite a few massive blackouts over the past 40 years, three of which have occurred in the past nine years. Power outages cost American businesses alone at least $150 billion each year [1]. For example:

- In 2000, the one-hour outage that hit the Chicago Board of Trade resulted in $20 trillion in trades delayed [1].
• Sun Microsystems estimates that a blackout costs the company $1 million every minute [1].

• The Northeast blackout of 2003 resulted in a $6 billion economic loss to the region [1]. More blackouts are occurring due to “poor visibility” on the part of grid operators. This issue of blackouts has wider reaching implications than just waiting to use the microwave. Some of its effects are perishable food spoiling, traffic lights going dark, and credit card transactions rendered inoperable. Even a short regional blackout can have such effects. America is relying on a centrally planned and controlled infrastructure created largely before the age of microprocessors that limits flexibility.

Efficiency: If the grid were just 5% more efficient, the energy savings would equate to permanently eliminating the fuel and greenhouse gas emissions from 53 million cars [1].

The problem is compounded by a spur of growth of the digital sector. In the 1980s, electrical load from electronic equipment such as computerized systems and automated manufacturing was limited. In the 1990s, chip share grew to roughly 10% [1]. Today, load from chip technologies and automated manufacturing has risen to 40%, and the load is expected to increase to more than 60% by 2015 [1]. By having a better demand response system, it is estimated that tens of billions of dollars will be saved by avoiding the need to build new power plants and transmission lines.
Affordability: The cost of electricity has increased visibly in recent years due to removal of rate caps. The costs associated with an underperforming grid are unaccounted for and remain largely unreported. Energy prices will rise but the trajectory of future cost increases will be more gradual post-Smart Grid as customers will be provided more options to manage electricity consumption thus controlling their own utility bills.

Security: The Northeast Blackout of 2003 – the largest in US history – caused panic among many people. The interdependencies of various grid components brought about a domino effect bringing to halt the banking system, communications, and traffic and security systems. The Smart Grid will be more resistant to attacks than the traditional grid and also move towards independence from foreign energy sources which are highly volatile.

Environment/Climate Change: The United States accounts for only 4% of the world’s population and produces 25% of its greenhouse gases [1]. Half of the country’s electricity is still produced by burning coal which is a major contributor to global warming. It is necessary to integrate clean, renewable sources of energy like solar, wind and geothermal into the nation’s grid. However, without appropriate enabling technologies linking them to the grid, their potential will not be fully realized. Table 1-1[1] compares the traditional grid to Smart Grid and acts as a summary as to why we need a Smart Grid in the first place.
### Table 1-1: Comparison of Traditional Grid vs. Smart Grid [1]

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Today’s Grid</th>
<th>Smart Grid</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables active participation by consumers</td>
<td>Consumers are uninformed and non-participative with power system</td>
<td>Informed, involved, and active consumers - demand response and distributed energy resources.</td>
</tr>
<tr>
<td>Accommodates all generation and storage options</td>
<td>Dominated by central generation- many obstacles exist for distributed energy resources interconnection</td>
<td>Many distributed energy resources with plug-and-play convenience focus on renewable sources</td>
</tr>
<tr>
<td>Enables new products, services and markets</td>
<td>Limited wholesale markets, not well integrated - limited opportunities for consumers</td>
<td>Mature, well-integrated wholesale markets, growth of new electricity markets for consumers</td>
</tr>
<tr>
<td>Provides power quality for the digital economy</td>
<td>Focus on outages - slow response to power quality issues</td>
<td>Power quality is a priority with a variety of quality/price options</td>
</tr>
<tr>
<td>Optimizes assets &amp; operates efficiently</td>
<td>Little integration of operational data with asset management - business process silos</td>
<td>Greatly expanded data acquisition of grid parameters - focus on minimizing impact to consumers</td>
</tr>
<tr>
<td>Anticipates and responds to system disturbances</td>
<td>Responds to prevent further damage- focus is on protecting assets following fault</td>
<td>Automatically detects and responds to problems so as to focus on minimizing impact to consumers</td>
</tr>
<tr>
<td>Operates resiliently against attack and natural disaster</td>
<td>Vulnerable to malicious acts of terror and natural disasters</td>
<td>Resilient to attack and natural disasters with rapid restoration capabilities</td>
</tr>
</tbody>
</table>
1.3 Smart Grid

Smart Grid is an electricity infrastructure consisting of devices installed at homes and businesses throughout the electricity distribution grid for the purpose of energy monitoring which utilizes the computer, networking and communications technologies all the way from the generation, transmission and distribution of electricity to consumer appliances and equipments [4]. Smart Grid brings together the utility and the internet. Smart grid delivers electricity from suppliers to consumers using two-way digital communications to control appliances at consumers' homes. It provides consumers with the ability to use electricity more efficiently while at the same time providing utilities with the ability to detect problems on their systems and operate them more efficiently. To add monitoring, analysis, control, and communication capabilities to the national electrical delivery system to maximize the throughput of the system while reducing the energy consumption is the basic concept of Smart Grid is shown in Figure 1-2 [3].
In Figure 1-2 [3], the sensors are used to detect variances in demand and also detect fluctuations and disturbances and send information signals to the demand management systems. The demand management system generates decision signals so as to increase or decrease the electricity generation at the generators and these signals are sent out to the processors. The processors would execute these instructions and take appropriate actions instantaneously such as triggering the system to isolate the micro-grid that is experiencing a disturbance or increase power generation at the generators. The storage could be used to store the extra energy generated at off-peak times. Storage acts as a buffer to supplement the generators. Also, based on customized power profiles registered
by the consumers with the utilities, these processors could initiate shutting down of appliances or manage the appliances according to the power profiles. Similarly, the power profiles could be a preset recommended profile set by the utilities, or a customized profile from the consumer wherein, the consumer specifies his requirements based on his/her need and the price information from the utilities.

Today the grid transmits information one way - from utility to customer. Power companies charge the same rate for every kilowatt-hour of electricity that's consumed, even though the cost of generating electricity changes dramatically during the day. Since consumers don't see how much power they are using or how much it costs in real time to generate it, they have little incentive to conserve energy or shift their use to off-peak hours. Smart Grid allows utilities to move electricity around the system as efficiently and economically as possible. It will also allow the homeowner and business to use electricity as economically as possible. When power is least expensive the user can allow the smart grid to turn on selected home appliances such as washing machines or heaters that can run at predetermined hours. At peak times it could turn off selected appliances to reduce demand as shown in Figure 1-3 [5].
Figure 1-3: How Smart Grid works [5].

Figure 1-3 [5] shows the working of Smart Grid so that it is easy to understand. To understand it better let us take an example: One consumer may want to keep his/her house set at 65 degrees F in the winter time when prices are high, but one might be willing to increase one’s thermostat to 70 degrees F if prices are low. Similarly a customer may want to dry clothes or vacuum the house for 10 cents per kilowatt-hour late in the evening when prices are low instead of 20 cents per kilowatt-hour at in the afternoon when demand and price are at their peak. The consumer will have the choice and flexibility to manage his/her electrical use while minimizing costs. Smart Grid builds
on many of the technologies already used by electric utilities but it also adds communication and control capabilities to optimize the operation of the entire electrical grid.

1.4 Literature Review

In this section, we discuss work done on Home Area Networks by other organizations and various ways in which they are looking at security issues.

The ZigBee Alliance, Z-Wave Alliance and the Wi-Fi Alliance have each conducted detailed analysis of ZigBee, Z-Wave and Wi-Fi technologies respectively regarding it’s suitability for Smart Grid taking in factors such as security, scalability and reliability.

Other organizations like Trilliant Inc. have come up with complete Smart Grid communication solutions to provide homes with a solution to meet their Smart Grid networking demands. One of the solutions that Trilliant Inc. has implemented to the meet the demand-side management is a SecureMesh HAN solution which enables smart grid home automation solutions [6].

UCA International Users Group is a non-profit corporation which consists of many task forces, one of which is OpenHAN. OpenHAN research is mostly focused on providing common specifications and requirements for a home area network protocols. It has
published the SRS document for Home Area Networks which seeks to ensure that Home Area Networks in Smart grid have a competitive market place by driving down costs, increasing interoperability, and maximizing longevity and maintainability.

National Institute of Standards and Technology (NIST) through its Cyber Security Working Group (CSWG) has defined a set of common security requirements for existing and upcoming home area networks [7].

An IEEE paper by the title of “Home Area Network Technology Assessment for Demand Response in Smart Grid Environment” by Md. Zahurul Hu, Prof. Syed Isla [8] carried out a brief assessment of different technologies such as ZigBee, Z-Wave, Wi-Fi, HomePlug etc as possible candidates for home area networks in smart grid. This project covers present and potential security issues in various communication protocols in Home Area Networks such as ZigBee, Z-Wave and Wi-Fi. It also discusses few countermeasures that help reduce the effect of the threat involved and also recommends the most suitable protocol based on the analysis.

1.5 Scope of the Project
The aim of this project is to provide a deep insight on a few communication protocols used in home area networks for Smart Grid. The scope also includes analysis of the protocols, comparisons and a recommendation on the best suitable protocol that could be
implemented in home area networks. Chapter 2 emphasizes on home area network, its requirements for Smart Grid and its significance in Smart Grid. Chapter 3 acquaints us with the underlying Medium Access Control protocols and standards that are in contention for implementation in home area networks. Chapter 4 discusses the different kinds of protocols that find their way into home area network. In Chapter 5 we will discuss the security issues and vulnerabilities associated with the protocols and standards discussed in Chapter 3 and Chapter 4. Chapter 6 lists the counter measures and best practices for the protocols or standards discussed in Chapter 3 and Chapter 4. Some of these countermeasures do not provide complete security and hence requires more research; Chapter 7 would identify such research areas in home area networks.
2.1 What is a Home Area Network?

A home area network (HAN) is used for communication between digital devices used in a typical home. It usually is a small number of personal computers and accessories, such as printers and mobile computing devices. We will discuss the role of a home area network in smart grid in the next section.

2.2 Role of Home Area Networks in Smart Grid

A home is the area where people are most affected by smart grid. The HAN is a subsystem within the Smart Grid dedicated to demand-side management (DSM), including energy efficiency and demand response. Real time electricity usage and cost information would need to be relayed to consumers so that they can know the costs and make informed decisions. The appliances need to relay information about how much electricity is being used to the utility so that demand response can be calculated. This is a vital piece of information since prices are calculated based on demand. At peak demand, the cost of electricity is at its highest and low when demand is low. Consumers thus have an incentive to run home appliances at non-peak times.

Figure 2-1[10] shows the sort of communication that takes place between a consumer and a utility. The appliances in a home relay that information to the utility using home area
networks (HAN). Meters made smart with embedded intelligence may be used to connect the home to the utility. This allows the utility to change rates in hourly or even 15 minute intervals. This direct communication between appliances and the meter is made possible by home area networks and leads to greater transparency and cooperation to reduce peak loads. By reducing demand during peak times, building new generating plants can be delayed, perhaps even indefinitely since renewable power sources are coming online.

Figure 2-1: Communication between Utility and Consumer [10]
Figure 2-2 [11] shows the various appliances in a home such as washers, dryers, refrigerators. The various devices communicate to the smart meter using home area networks. All these smart devices need a way to talk to one other. In the home, communication will likely take place over a home area network (HAN) in which each appliance is a node. Plug-in vehicles are an important part of Smart Grid. A handful of vehicles draw as much if not more power than a large home with all appliances home. This is an area of concern. But, the advantage is that car batteries can also act as reservoirs of energy storage. Making everything work together requires standards, especially when the grid consists of close to 3,000 separate utilities that operate on their own. The smart grid is a system of systems, each needing to interoperate. Connecting the refrigerator, to the smart meter-access point, to the electrical substations and even power-generating systems, requires interoperability at each point [11]. In the home, appliances from different manufacturers will need a common protocol to communicate on the HAN and with the smart meter. NIST (National Institute of Standards and Technology) is an organization that is charged with fostering smart grid standards and encouraging interoperability.
Appliances can also be smart. Manufacturers are ready to begin inserting chips to collect and report usage data so homeowners will know the power consumption of each device. Any other device will be programmable to run only when electricity is cheapest. The smart meter, when alerted by the utility, sends a message to the refrigerator for it to go into energy-saving mode, delaying freezer defrost cycles or sends a message to the thermostat to delay heat/cool cycles. The sequence in Figure 2-3 [12] shows the working of demand response in a smart grid and the role played by home area networks in reducing peak periods.
Figure 2-3: An example of the role of HAN in demand – response [12].
These industries have implemented a huge variety of networking technologies, open and proprietary, wired and wireless. The leaders in this area include BACnet, HomePlug 6LowPAN and ZigBee, plus semi-proprietary solutions like LONtalk, Insteon, and Z-Wave; more traditional (but costly and power-hungry) open standards like Ethernet and Wi-Fi; and popular legacy protocols such as X10. Such diversity and lack of interoperability has presented difficulties to the vendors in these markets previously, but the problem has been exacerbated by the deployment of AMI and other Smart Grid applications.

There are three main wireless standards - low power Z-Wave, ZigBee and Wi-Fi - plus six powerline options for home appliance networks [33]. The above mentioned communication protocols will be discussed in chapter 4. However, before that, the underlying MAC protocols and standards that are associated with each of the protocols will be discussed in chapter 3.
Chapter 3

UNDERLYING MAC PROTOCOLS AND STANDARDS

3.1 IEEE 802.15.4

3.1.1 Introduction to IEEE 802.15.4

In this chapter we will be discussing the need for the 802.15.4 and its role in Smart Grid. Further, we will also be describing the architecture of the IEE 802.15.4 standard along with the security services provided by the standard for use by the higher layer applications. A brief overview of the general functions of a Low-Rate Wireless Personal Area Networks (LR-WPAN) is also covered which includes information on the superfame structure, the data transfer model, the frame structure, robustness, power consumption considerations, and security.

Until a few years back, most activity in network technology focused on high throughput which meant high bandwidth. However, some applications in the following areas such as Home automation: Heating, ventilation, air conditioning, security, lighting and the control of objects.

Automotive: Automotive sensing, such as tire pressure monitoring.

Agriculture: Sensing of soil moisture, pesticide, herbicide, and pH levels.

Industrial: Monitoring machines etc have relaxed throughput requirements with low power consumption and low cost. Networking standards that existed at that point of time were not suitable due to high complexity, power implications and high cost. A new
A standard was required to address these problems. A task group was created to come up with a standard to address the above problems. The goal of this group was to provide a standard with ultra-low complexity, cost and power for low-data-rate wireless connectivity among inexpensive fixed, portable, and moving devices. In order to achieve the low power and low cost goals established by IEEE 802.15.4 Standard for Low-Rate Wireless Personal Area Networks (LR-WPAN) the following approaches were taken:

- Reduction in the data transfer rate.
- Reduction in the transceiver duty cycle and frequency of data transmissions.
- Reduction of the frame overhead.
- Reduction of complexity.
- Reduction of range.
- Strict power management mechanisms (power-down and sleep modes).

The above characteristics are perfect for use in home area networks in Smart Grid where battery life has to be conserved as changing batteries in home products every few months is impractical. Also, latency is not a problem since data is not time sensitive. ZigBee builds on top of the IEEE 802.15.4-2003 standard which makes ZigBee a perfect candidate for Home Area Networks (HAN) due to the above characteristics. HAN is an essential tool in the Smart Grid palette of offerings allowing Smart Grid applications to communicate intelligently with multiple appliances in a home. Figure 3-1 [13] below is a summary of IEEE 802.15.4 characteristics.
Figure 3-1: A summary of IEEE 802.15.4 characteristics [13]

The IEEE 802.15 working group defines three classes of Wireless Personal Area Networks (WPANs) characterized by data rate, power usage, and quality of service [14]

- **802.15.1**: Medium-rate: Voice applications, PDAs, etc.
- **802.15.3**: High-data-rate, High quality of service. Good for multi-media applications.
- **802.15.4**: Low data-rate, lower cost, low power, and lower quality of Service (QoS) than 802.15.1.

A comparison of IEEE 802.15.4 with respect to other IEEE standards is shown below

<table>
<thead>
<tr>
<th>Property</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Raw data rate</td>
<td>868 MHz: 20 kb/s; 915 MHz: 40 kb/s; 2.4 GHz: 250 kb/s</td>
</tr>
<tr>
<td>Range</td>
<td>10 - 20 meters</td>
</tr>
<tr>
<td>Latency</td>
<td>Down to 15 ms</td>
</tr>
<tr>
<td>Channels</td>
<td>868 MHz: 1 channel; 915 MHz: 10 channels; 2.4 GHz: 16 channels</td>
</tr>
<tr>
<td>Frequency band</td>
<td>Two PHYs: 868 MHz/915 MHz and 2.4 GHz</td>
</tr>
<tr>
<td>Addressing</td>
<td>Short 16-bit or 64-bit IEEE</td>
</tr>
<tr>
<td>Channel access</td>
<td>CSMA-CA and slotted CSMA-CA</td>
</tr>
<tr>
<td>Temperature</td>
<td>Industrial temperature range -40 to +85 C</td>
</tr>
</tbody>
</table>
3.1.2 IEEE 802.15.4 Architecture

The Low Rate - Wireless Personal Area Network (LR-WPAN) architecture is defined in terms layers. Each layer offers services to the higher layers. The layout of the layers is based on the open systems interconnection (OSI) seven-layer model.

An LR-WPAN device comprises a PHY and a MAC sub-layer. The PHY layer contains the radio frequency (RF) transceiver along with its low-level control mechanism. A MAC sub-layer provides access to the physical channel for all types of transfer. A graphical representation is shown in Figure 3-3 [16]. The upper layers consist of a network layer, which provides network configuration, manipulation, and message routing, and an application layer, which provides the intended function of the device [16]. The scope of this standard does not cover the definition of these layers. An IEEE 802.2 Type 1 logical
link control (LLC) can access the MAC sub-layer through the service specific convergence sub-layer (SSCS) which are again out of the scope for this standard. The LR-WPAN architecture is implemented either as embedded devices or as devices requiring the support of an external device such as a PC [16].

Figure 3-3: LR-WPAN device architecture [16].

3.1.2.1 PHY

The PHY is responsible for the following tasks:

- Activation and deactivation of the radio transceiver: The radio transceiver can operate in one of the following three states: transmitting, receiving or sleeping.
The radio is turned ON or OFF based on the request of the MAC sub-layer. According to the standard, the turnaround time from transmitting to receiving and vice versa should be no more than 12 symbol periods where each symbol corresponds to 4 bits.

- **Energy Detection (ED):** This is an estimation of the received signal power within the bandwidth of an IEEE 802.15.4 channel. There is no signal identification or decoding on the channel involved. The energy detection time should be equal to 8 symbol periods. This measurement of energy detection is used by the Network Layer as a part of channel selection algorithm or for the purpose of Clear Channel Assessment (CCA), to determine if the channel is busy or idle [16].

- **Link Quality Indication (LQI):** This is a measurement of the strength or quality of a received packet. This measurement may be implemented using receiver ED to detect the quality of the signal on the receiving device.

- **Clear Channel Assessment (CCA):** It is an evaluation of the activity state in the medium: busy or idle. The CCA is performed in three operational modes:
  - **Energy Detection mode:** If the detected energy is above the ED threshold, a busy medium is reported by the CCA.
  - **Carrier Sense mode:** A busy medium is reported by the CCA only if it detects a signal with the modulation of IEEE 802.15.4 which may be higher or lower than the ED threshold.
o Carrier Sense with Energy Detection mode: This is a combination of the abovementioned techniques. A busy medium is reported only if it detects a signal with the modulation and the spreading characteristics of IEEE 802.15.4 and with energy above the ED threshold.

- Channel Frequency Selection: There are 27 different wireless channels defined by IEEE 802.15.4. Each network can support only part of the channel set. Therefore, the physical layer should be able to tune its transceiver into a specific channel when requested by a higher layer.

Two services are provided by the Physical layer (PHY):

PHY data service: It enables the transmission and reception of PHY protocol data units (PPDU’s) across the physical radio channel.

PHY management service: It is responsible for maintaining a database of managed objects pertaining to the PHY. This service is managed by the PHY management entity (PLME). The radio operates at one of the following license-free bands:

- 868–868.6 MHz (e.g., Europe),
- 902–928 MHz (e.g., North America) or
- 2400–2483.5 MHz (worldwide).

3.1.2.2 MAC Layer

The MAC sub-layer handles all access to the physical radio channel and is responsible for the following tasks:
- Generating network beacons if the device is a coordinator.
- Synchronizing to the beacons.
- Supporting PAN association and disassociation.
- Supporting device security.
- Employing the CSMA-CA mechanism for channel access.
- Handling and maintaining the GTS mechanism.
- Providing a reliable link between two peer MAC entities.

The MAC protocol supports two operational modes:

- Non beacon-enabled mode: In the non-beacon enabled mode, there are neither beacons nor superframes. Medium access is ruled by an unslotted CSMA/CA mechanism which is discussed in further sections.

- Beacon-enabled mode: In this mode, beacons are periodically sent by the coordinator device to synchronize nodes that are associated with it, and to identify the personal area network (PAN). A beacon frame delimits the beginning of a superframe defining a time interval during which frames are exchanged between different nodes in the PAN. Medium access is ruled by Slotted CSMA/CA. The beacon-enabled mode also enables the allocation of contention free time slots, called Guaranteed Time Slots (GTS) for low latency nodes that require guaranteed bandwidth.

Two services are provided by the MAC layer:
MAC data service: It enables the transmission and reception of MAC protocol data units (MPDU’s) across the PHY data service. The features offered by the MAC sub-layer are beacon management, channel access, GTS management, frame validation, acknowledged frame delivery, association, and disassociation [16].

MAC management service: It maintains a database of managed objects pertaining to the MAC sub-layer. This database is referred to as the MAC sub-layer PIB. The entity that provides this service is the MAC management entity (MLME). This entity provides the service interfaces through which layer management functions may be invoked.

3.1.2.2.3 Superframe Structure

The Low-Rate Wireless Personal Area Network (LR-WPAN) standard allows the use of a superframe structure although it is optional.

![Superframe Structure without guaranteed time slots](image)

**Figure 3-4: Superframe Structure without guaranteed time slots [16].**

The format of the superframe is defined by the coordinator. The superframe is divided into 16 equally sized slots and is bounded by network beacons. It is sent by the
coordinator. In the first slot of each superframe, the beacon frame is transmitted. A coordinator may turn off the beacon transmissions, if a coordinator does not wish to use a superframe structure. The beacons are used to synchronize the attached devices and to describe the structure of the superframes. The beacons are also used to identify the PAN. Devices that wish to communicate during the contention access period (CAP) between two beacons compete with other devices using a slotted CSMA-CA mechanism which is explained in detail in further sub chapters. All transactions have to be completed by the time of the next network beacon.

Figure 3-5: Superframe structure with guaranteed slots [16].

The superframe can have an active and an inactive portion. During the inactive portion, the coordinator does not interact with its PAN and enters a low-power mode. For low-latency applications or applications requiring specific data bandwidth, the PAN coordinator dedicates portions of the active superframe to that application [16]. These portions are called guaranteed time slots (GTSs). The GTSs form the contention-free
period (CFP), which always appears at the end of the active superframe starting at a slot boundary immediately following the CAP, as shown in Figure 3-5 [16]. The PAN coordinator can allocate up to seven of these GTSs. A GTS may occupy more than one slot period. Nevertheless, a sufficient portion of the CAP remains for contention-based access of other networked devices or new devices that wish to join the network. All contention-based transactions are completed before the CFP begins. Each device transmitting in a GTS has to ensure that its transaction is complete before the time of the next GTS or the end of the CFP.

3.1.2.3 Data Transfer Model

There are three types of data transfer transactions. In the first one data is transferred to a coordinator from a device. In the second model, data is transferred from a coordinator to a device. In the third model, data is transferred between two peers. Only two of these transactions are used in a star topology since data is only transferred to and from the coordinator. All three transactions are used in a peer-to-peer technology since data may be exchanged between any two devices on the network. The mechanisms used may again differ based on whether the network supports the transmission of beacons. Low latency devices like PC peripherals use a beacon-enabled network. If no such devices exist on the network then beacon may not need to be used for normal data transfer. The beacon may however still be needed for network association.
3.1.2.3.1 Data Transfer to a Coordinator

Figure 3-6 [16] is a visual description of the mechanism by which data is transferred from a device to a coordinator. If a device is to transfer data to a coordinator in a beacon-enabled network, it listens for the network beacon [16]. The device synchronizes to the superframe structure when the beacon is found. The device then transmits its data frame to the coordinator at the appropriate time using slotted carrier sense multiple access – collision avoidance (CSMA-CA). An acknowledgement frame is sent by the coordinator to acknowledge successful reception of data.

![Figure 3-6: Communication to a coordinator in a beacon-enabled network [16].](image)

A device wishing to transfer data in a non beacon-enabled network simply transmits its data frame to the coordinator using unslotted CSMA-CA. An optional acknowledgement
frame is sent by the coordinator to acknowledge successful reception of data, thus completing the transaction. Figure 3-7 [16] is a visual description of the aforementioned sequence of events.

Figure 3-7: Communication to a coordinator in a non beacon-enabled network [16].

3.1.2.3.2 Data Transfer from a Coordinator

In a beacon-enabled network, when the coordinator wished to transfer data, it indicates that the data message is pending in the network beacon. The device receiving data from the coordinator periodically listens to the network beacon. If it finds that a message is pending, it transmits a MAC command requesting the data using slotted CSMA-CA. The coordinator then transmits an optional acknowledgement to relay a successful reception message. The pending data frame is sent using slotted CSMA-CA. The device then transmits an acknowledgement frame acknowledging the successful reception of data,
thus completing the transaction. The message is removed from the pending messages in the beacon after the arrival of the acknowledgement frame. Figure 3-8 [16] shows the mechanism by which data is transferred from a coordinator to a device.

Figure 3-8: Communication from a coordinator in a beacon-enabled network [16].

When a coordinator wishes to transfer data to a device in a non beacon-enabled network, it stores the data for the appropriate device to make contact and request the data. A device may make contact by transmitting a MAC command requesting the data, using unslotted CSMA-CA, to its coordinator at an application-defined rate. The coordinator acknowledges the successful reception of the data request by transmitting an acknowledgment frame. If data are pending, the coordinator transmits the data frame,
using unslotted CSMA-CA, to the device. If data are not pending, the coordinator transmits a data frame with a zero-length payload to indicate that no data were pending. The device acknowledges the successful reception of the data by transmitting an acknowledgment frame. The transaction is complete. Figure 3-9 is a visual representation of the sequence explained above.

![Communication from a coordinator in a non beacon-enabled network](image)

**Figure 3-9:** Communication from a coordinator in a non beacon-enabled network [16].

### 3.1.2.3.3 Peer-to-Peer Data Transfer

In a peer-to-peer personal area network, every device communicates with all other devices. Effective communication between the devices requires constant communication or synchronization.
3.1.2.4 Frame Structure

The frame structures have been designed to keep the complexity to a minimum while at the same time making them sufficiently robust for transmission on a noisy channel [16]. Each successive protocol layer adds to the structure with layer-specific headers and footers [16]. The LR-WPAN defines four frame structures:

A beacon frame: Used by a coordinator to transmit beacons.

A data frame: Used for all transfer of data.

An acknowledgment frame: Used for confirming successful frame reception.

A MAC command frame: Used for handling all MAC peer entity control transfers.

The structure of each of the four frame types is described in 4.4.3.1 through 4.4.3.4. The diagrams in these sub-clauses illustrate the fields that are added by each layer of the protocol. The packet structure illustrated below the PHY represents the bits that are actually transmitted on the physical medium.

3.1.2.4.1 Beacon Frame

A beacon frame originates from the MAC sub-layer. A coordinator transmits network beacons in a beacon-enabled network. The MAC service data unit (MSDU) contains the superframe specification, pending address specification, address list, and beacon payload fields [16]. The MSDU contains a MAC header (MHR) as a prefix and MAC footer (MFR). The MHR contains the MAC frame control fields, beacon sequence number (BSN), and addressing information fields [16]. The MFR contains a 16 bit frame check
sequence (FCS). The MHR, MSDU, and MFR together form the MAC beacon frame (i.e., MPDU).

The MPDU is then passed to the PHY as the PHY beacon packet payload also called the PHY service data unit (PSDU). The PSDU has a synchronization header (SHR) as a prefix, which in turn contains the preamble sequence and start-of frame delimiter (SFD) fields, and a PHY header (PHR) containing the length of the PSDU in octets. The preamble sequence enables the receiver to achieve symbol synchronization. The SHR, PHR, and PSDU together form the PHY beacon packet, (i.e., PPDU) [16]. Figure 3-10 [16] shows the structure of the beacon frame, which originates from the MAC sub-layer.

<table>
<thead>
<tr>
<th>Octets:</th>
<th>2</th>
<th>1</th>
<th>4 or 10</th>
<th>2</th>
<th>k</th>
<th>m</th>
<th>a</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MAC sublayer</strong></td>
<td>Frame Control</td>
<td>Sequence Number</td>
<td>Addressing Fields</td>
<td>Superframe Specification</td>
<td>GTS Fields</td>
<td>Pending Address Fields</td>
<td>Beacon Payload</td>
<td>FCS</td>
</tr>
<tr>
<td></td>
<td>MHR</td>
<td>MSDU</td>
<td>MFR</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Octets:</th>
<th>4</th>
<th>1</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PHY layer</strong></td>
<td>Preamble Sequence</td>
<td>Start of Frame Delimiter</td>
<td>Frame Length</td>
</tr>
<tr>
<td>SHR</td>
<td>PHR</td>
<td>PSDU</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Octets:</th>
<th>13</th>
<th>10</th>
<th>k</th>
<th>m</th>
<th>n</th>
</tr>
</thead>
</table>

PPDU

Figure 3-10: Schematic view of the beacon frame [16].

3.1.2.4.2 Data Frame

The data payload is passed to the MAC sub-layer. It is referred to as the MSDU. The MSDU is prefixed with an MHR and appended with an MFR as a suffix. The frame
control, sequence number, and addressing information fields is contained within the MHR. The MFR is composed of a 16 bit FCS. The MHR, MSDU, and MFR together form the MAC data frame also referred to as the MPDU [16]. The MPDU is passed to the PHY as the PHY data frame payload also referred to as the PSDU [16]. The PSDU is prefixed with an SHR, containing the preamble sequence and start of frame delimiter fields (SFD), and a PHR which contains the length of the PSDU in octets. The preamble sequence and the data start of frame delimiter (SFD) enable the receiver to achieve symbol synchronization. The SHR, PHR, and PSDU together form the PHY data packet also referred to as the PPDU [16]. Figure 3-11 [16] shows the structure of the data frame, which originates from the upper layers.

![Schematic view of the data frame](image)

Figure 3-11: Schematic view of the data frame [16].
3.1.2.4.3 Acknowledgment Frame

The acknowledgement frame originates from the MAC sub-layer. It is constructed from an MHR and a MFR. The MAC frame control and data sequence number fields are contained within the MHR. The MFR is composed of a 16 bit FCS. The MHR and MFR together form the MAC acknowledgment frame also referred to as the MPDU) [16]. The MPDU is passed down to the PHY as a PHY acknowledgement frame payload which is the PSDU. The PSDU is then prefixed with the SHR, containing the preamble sequence and SFD fields, and the PHR containing the length of the PSDU in octets [16]. The SHR, PHR, and PSDU together form the PHY acknowledgment packet also referred to as the PPDU [16]. Figure 3-12 [16] shows the structure of the acknowledgment frame.

![Figure 3-12: Schematic view of the acknowledgement frame](image-url)

Figure 3-12: Schematic view of the acknowledgement frame [16].
3.1.2.4.4 MAC Command Frame

The command type field and command specific data are called the command payload. The command payload is contained within the MSDU. The MSDU is then prefixed with a header and footer called the MHR and MFR respectively. The MAC frame control, data sequence number, and addressing information fields are contained within the MHR. The MFR is a 16 bit FCS. The MAC command frame which is MPDU is formed by the MHR, MSDU and the MFR together. Figure 3-13 [16] shows the structure of the MAC command frame. The MAC command frame originates from the MAC sub-layer.

![Schematic view of the MAC command frame](image)

3.1.2.4.4.1 Robustness

Various mechanisms are used to ensure robustness in the data transmission. These mechanisms are the CSMA-CA mechanism, frame acknowledgment, and data verification.
3.1.2.4.4.1.2 CSMA-CA Mechanism

Two types of channel access mechanisms are used in LR-WPAN depending on the network configuration. Unslotted CSMA-CA channel access mechanisms are used by nonbeacon-enabled networks. A device waits for a random period of time each time it wishes to transmit data frames or MAC commands. If the channel is idle following the random backoff, the device transmits the data. If the channel is not idle following the random backoff, the device waits for another random period before trying to access the channel and transmit the data again. Acknowledgment frames however are sent without using a CSMA-CA mechanism. Slotted CSMA-CA channel access mechanisms are used by beacon-enabled networks. Here the backoff slots are aligned with the start of the beacon transmission. The device that wishes to transmit data frames during the CAP locates the boundary of the next backoff slot and then waits a random number of backoff slots. Following the random backoff, if the channel is busy, the device waits for another random number of backoff slots. If the channel is idle, the device transmits data on the next available backoff slot boundary. Both acknowledgement and beacon frames are sent without using a CSMA-CA mechanism. The CSMA-CA algorithm is used before the transmission of data or MAC command frames within the contention access period (CAP). The CSMA-CA algorithm is not used for transmission of beacon, acknowledgement or data frames transmitted in the contention free period (CFP). There are two CSMA-CA mechanisms.
Slotted CSMA-CA mechanism: This mechanism is used for transmissions in the CAP of the superframe by the MAC sub-layer when beacons are used in the personal area network (PAN). The backoff periods of one device are not related in time to the backoff periods of any other device in the PAN. The MAC sub-layer ensures that the PHY commences all of its transmissions on the boundary of a backoff period.

Unslotted CSMA-CA mechanism: This mechanism is used for transmission by the MAC sublayer when beacons are not used in the PAN or if a beacon cannot be located in a beacon-enabled network. The backoff period boundaries of every device in the PAN are aligned with the superframe slot boundaries of the PAN coordinator in slotted CSMA-CA.

The algorithm is implemented using units of time called backoff periods in both mechanisms. Every device maintains three variables for each transmission attempt:

$NB$: $NB$ is the number of times the CSMA-CA algorithm was required to backoff while attempting the current transmission. This value is initialized to 0 before each new transmission attempt.

$CW$: $CW$ is the contention window length. It defines the number of backoff periods that need to be clear of channel activity before the transmission can begin. This value is initialized to 2 before every transmission attempt and reset to 2 each time the channel is assessed to be busy. The $CW$ variable is only used for slotted CSMA-CA.

$BE$: $BE$ is the backoff exponent. This is related to how many backoff periods a device will wait before attempting to assess a channel. Both in unslotted systems and slotted
systems with macBattLifeExt set to FALSE, BE is initialized to the value of \textit{macMinBE}. In slotted systems with macBattLifeExt set to TRUE, this value is set to the minimum value between 2 and the value of MAC sub-layer constant namely macMinBE. If macMinBE is set to 0, collision avoidance will be disabled during the first iteration of this algorithm. Although the receiver of the device is enabled during the channel assessment portion of this algorithm, the device discards any frames received during this time.
Figure 3-14: CSMA-CA Algorithm [17].

The slotted CSMA/CA can be summarized in five steps:

Step 1: The NB, CW and BE are initialized. The number of backoffs and the contention window are initialized (NB = 0 and CW = 2). The backoff exponent is initialized to BE =
2 or \( BE = \min (2, \text{macMinBE}) \) depending on the value of the Battery Life Extension MAC attribute. The field ‘macMinBE’ is a constant which is equal to 3 by default. The algorithm locates the boundary of the next backoff period after the initialization [17].

Step 2: A random waiting delay is calculated for collision avoidance. The algorithm starts counting down a random number of Backoff periods (BPs) uniformly generated within \([0, 2^{BE} - 1]\). The countdown starts at the boundary of a BP. To disable the collision avoidance procedure at the first iteration, \( BE \) must be set to 0, and thus the waiting delay is null and the algorithm goes directly to Step 3 [17].

Step 3: The algorithm performs a Clear Channel Assessment (CCA) operation at the BP boundary to assess channel activity as soon as the timer expires. The algorithm goes to Step 4 if the channel is busy. If the channel is idle, the algorithm goes to Step 5 [17].

Step 4: If the channel is busy, \( CW \) is re-initialized to 2. \( NB \) and \( BE \) are incremented. \( BE \) must not exceed \( \text{aMaxBE} \), which has a default value of 5. The probability for having greater backoff delays are increased by incrementing \( BE \). If the maximum number of backoffs \( (NB = \text{macMaxCSMABackoffs} = 5) \) is reached, the algorithm reports a failure to the higher layer. Otherwise, it goes back to Step 2 and the backoff operation is restarted [17].

Step 5: If the channel is idle the \( CW \) value is decremented. If \( CW = 0 \) in Step 3, the CCA is repeated. This ensures performing two CCA operations to prevent potential collisions of acknowledgement frames. If the channel is again sensed as idle \( (CW = 0) \), the node
attempts to transmit. All the same, collisions may still occur if two or more nodes are transmitting at the same time [17].

The non-slotted CSMA/CA is discussed below. It is similar to the slotted version with a few exceptions.

Step 1: The CW variable is not used, since the non-slotted CSMA/CA has no need to iterate the CCA procedure after detecting an idle channel. Hence, in Step 3, if the channel is assessed to be idle, the MAC protocol immediately starts the transmission of the current frame. Second, the non-slotted CSMA/CA does not support macBattLifeExt mode and, hence, BE is always initialized to the macMinBE value [17].

Steps 2, 3 and 4: It is similar to the slotted CSMA/CA version. The only difference is that the CCA starts immediately after the expiration of the random backoff delay generated in Step 2 [17].

Step 5: The MAC sub-layer starts immediately transmitting its current frame just after a channel is assessed to be idle by the CCA procedure [17].

3.1.2.4.4.1.3 Frame Acknowledgment

A frame acknowledgement is used to acknowledge successful reception and validation of a data or a MAC command frame. Its use is optional. If the receiving device is unable to validate or receive the data, no acknowledgement is sent. The transmitting device waits for a certain period of time. If it does not receive the acknowledgement frame, it assumes
that the receiver did not get the message and retries the frame transmission. If there are still no acknowledgements from the receiver after several retries, the transaction can either be terminated or the transmitter can choose to retry. When the acknowledgment is not required, the originator assumes the transmission was successful [16].

3.1.2.4.4.1.4 Data Verification

In order to detect bit errors, an FCS mechanism, employing a 16 bit cyclic redundancy check (CRC), is used to protect every frame. This is a standard set by the International Telecommunication Union—Telecommunication Standardization Sector (ITU-T).

3.1.2.5 Power Consumption Considerations

Power consumption is of significant concern in many of the applications that use this standard. It is impractical to change or replace batteries at relatively short intervals. The standard was developed with this constraint in mind.

In many applications that use this standard, the devices will be battery powered where their replacement or recharging in relatively short intervals is impractical; therefore the power consumption is of significant concern. This standard was developed with the limited power supply availability in mind. Certain applications in some of these devices could potentially be mains powered. Battery-powered devices will require duty-cycling to reduce power consumption. Most of the operational life of such devices will be in sleep state. However, each device has to periodically listen to the RF channel in order to
determine whether a message is pending. This is the balance between battery consumption and message latency that has to be maintained. Mains-powered devices have the option of listening to the RF channel continuously since they do not have battery considerations.

3.1.2.6 IEEE 802.15.4 Security Overview

Four basic security services are provided by the link layer. They are

- Access Control: The link layer protocol prevents unauthorized parties from participating in the network.
- Message Integrity: If a message is altered while in transit, the receiver should be able to detect the tampering. It should also be able to authenticate that the sender is actually the device it claims to be.
- Message Confidentiality: Keep information secret from unauthorized parties.
- Replay Protection: Adversaries may eavesdrop on legitimate messages sent between two devices and play it back at another time. This should be prevented by the link layer.

The above services are discussed in more detail.

Access Control and message integrity: As mentioned above, the link layer provides access control services. Messages from unauthorized nodes should be detected and rejected by legitimate nodes. A secure network should also be able to detect messages that have been tampered with while in transit. Each packet is provided message
authentication and integrity with a Message Authentication Code []. IEEE 802.15.4 refers to the Message Authentication Code as a Message Integrity Code (MIC) to differentiate from Media Access Control (MAC). MIC is a cryptographically secure checksum. The sender and the receiver share a secret key. The MIC is computed with the secret key and the MIC is sent along with the packet. The receiving device shares the same secret key and re-computes the authentication code. If the two Message Integrity Codes are equal the packet is accepted by the receiver. Otherwise it is rejected. Forging of MIC must be difficult so as to protect authenticity. Access Control is achieved by using Access Control List (ACL). ACL stores the following fields.

Address: Address of the node it wants to communicate with.

Security Suite: The suite which is being used (AEC-CTR, AES-CCM-64, AES-CCM-128, etc).

Key: The 128 bit key used in the Analog Encryption Scheme (AES).

Last Initial Vector (IV) and Replay Counter: The Last IV is used by the source and the Replay Counter by the destination as a message ID in order to avoid reply attacks.

<table>
<thead>
<tr>
<th>Address</th>
<th>Security Suite</th>
<th>Key</th>
<th>Last IV</th>
<th>Replay Ctr</th>
</tr>
</thead>
</table>

Figure 3-15: Format of an ACL entry [18].

Confidentiality: Unauthorized parties should not gain access to secret or confidential data. This is achieved by encryption. An encryption scheme should prevent message
recovery. An encryption process should not be identical for any two invocations on the same message. This violates semantic security and results in the cipher texts being exactly the same. A nonce is used so that semantic security is not violated. A nonce plays the same role as a primary key in a database. It is unique and thus adds variation to the encryption scheme. The nonce is usually not encrypted so that the receiver may decrypt the message.

Replay Protection: A legitimate message between two nodes must not be allowed to be sent again at a later time. The MIC will be valid since the message is original and hasn’t been tampered with. Replay protection protects against such attacks [18]. The receiver assigns sequence numbers to each packet and the receiver rejects any packet with sequence numbers previously seen. IEEE 802.15.4-2003 specification supports the security suites listed in Table 3-1 [16].

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Null</td>
<td>No security</td>
</tr>
<tr>
<td>AES-CTR</td>
<td>Encryption only, CTR Mode</td>
</tr>
<tr>
<td>AES-CBC-MAC-128</td>
<td>128 bit MAC</td>
</tr>
<tr>
<td>AES-CBC-MAC-64</td>
<td>64 bit MAC</td>
</tr>
<tr>
<td>AES-CBC-MAC-32</td>
<td>32 bit MAC</td>
</tr>
<tr>
<td>AES-CCM-128</td>
<td>Encryption &amp; 128 bit MAC</td>
</tr>
</tbody>
</table>
Table 3-2 [16] paints a clearer picture of the security services available in each of the security suites.

Table 3-2: Security services offered by the various security suites supported by IEEE 802.15.4-2003 [16].

<table>
<thead>
<tr>
<th>Security suite</th>
<th>Security Services</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access control</td>
</tr>
<tr>
<td>None</td>
<td></td>
</tr>
<tr>
<td>AES-CTR</td>
<td>X</td>
</tr>
<tr>
<td>AES-CCM-128</td>
<td>X</td>
</tr>
<tr>
<td>AES-CCM-64</td>
<td>X</td>
</tr>
<tr>
<td>AES-CCM-32</td>
<td>X</td>
</tr>
</tbody>
</table>
The suites supported above can be broadly classified by the properties offered. Analog Encryption Scheme Counter Mode (AES-CTR) offers encryption only. Analog Encryption Scheme Cipher Block Chaining Message Authentication Code (AES-CBC-MAC) offers authentication only. Analog Encryption Scheme Counter with CBC-MAC (AES-CCM) provides both authentication as well as encryption.

3.1.2.6.1 AES-CTR Security Suite

This security suite provides only confidentiality. This is done by making use of AES block cipher [16] with counter mode.

The sender device breaks down the clear text data ‘d’ into ‘n’ 16-byte blocks d₁…dₙ. The cipher text Ci is computed by \( C_i = d_i \oplus E_k(x_i) \) where

\( E_k \) – Encryption Key

\( X_i \) – varying counter or nonce

\( C_i \) – Resulting cipher text
The receiving device requires the counter to decrypt the cipher text. The nonce is composed of a static flags field, the sender’s address and 3 other separate counters. The 3 counters are a 4 bit frame counter that identifies the packet, a 1 byte counter field, and a two byte block counter that numbers the 16 byte blocks within the packet [16]. The frame counter is maintained by the hardware radio. The value is incremented after encrypting every packet [16].

![Figure 3-16: Format of input \( (X_i) \) to the block cipher for AES-CTR and AES-CCM modes [16]](image)

The key counter is a one byte counter which is controlled by the application. The nonce should never be repeated in the lifetime of a key. The frame and the key counters prevent nonce reuse. The 2 byte block counter ensures that each block uses a different nonce value. To summarize, the sender includes the frame counter, key counter and the encrypted payload into the data payload field of the packet as shown in Figure 3-16 [16].

![Figure 3-17: Format of the data field in the AES-CTR Security Suite [18]](image)
3.1.2.6.2 AES-CBC-MAC Security Suite

This suite offers authentication protection only. The Message Authentication Code can only be computed by parties with the symmetric key. The Message Authentication Code protects both the data payload and the header. There are three different AES-CBC-MAC variants as the sender can compute 4, 8 or 16 byte Message Authentication Codes using the Cipher Block Chaining Message Authentication Code (CBC-MAC) algorithm. The longer the MAC, the lower is the chance that an adversary can achieve forgery by guessing an appropriate code [18]. For example, with an 8 byte MAC, an adversary has a $2^{-64}$ chance of forging the MAC [18]. The tradeoff is a larger packet size for increased protection against authenticity attacks [18]. The plaintext data is appended along with the Message Authentication Code by the sender. The receiving device verifies the Message Authentication Code by computing the Message Authentication Code and comparing it with the value that is included in the packet.

<table>
<thead>
<tr>
<th>variable</th>
<th>4/8/16 bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payload</td>
<td>MAC</td>
</tr>
</tbody>
</table>

Figure 3-18: Format of data field in the AES-CBC-MAC Security suite [18].

3.1.2.6.3 AES-CCM Security Suite

This security suite uses CCM mode for encryption and authentication [18]. CBC-MAC provides integrity protection for the header and the data payload. The data and the MAC
are then encrypted using the AES-CTR mode. Depending on the size of the Message Authentication Code that is computed using the CBC-MAC algorithm, AES-CCM has three variants similar to the AES-CBC-MAC suite.

![Figure 3-19: Format of data field in the AES-CCM Security suite [18].]

3.2 IEEE 802.11

3.2.1 Introduction to IEEE 802.11

A wireless LAN (WLAN) or wireless fidelity (Wi-Fi) is a data transmission system designed to provide location-independent network access between computing devices by using radio waves rather than a cable infrastructure [19].

The 802.11 specification [20] as a standard for wireless LANS was ratified by the Institute of Electrical and Electronics Engineers (IEEE). Like all IEEE 802 standards, the 802.11 standards focus on the bottom two levels the ISO model, the physical layer and link layer. The key motivation and benefit from Wireless LANs is increased mobility. Network users can move about almost without restriction and access the network from anywhere within the range of the network. The other advantage for WLAN is cost-
effective network setup for hard-to-wire locations as well as reduced cost of ownership due to minimal wiring and installation costs per device and user. WLANs liberate users from dependence on hard-wired access to the network backbone, giving them anytime, anywhere network access. This freedom to roam offers numerous user benefits for a variety of work environments. In the corporate enterprise, wireless LANs are usually implemented as the final link between the existing wired network and a group of client computers, giving these users wireless access to the full resources and services of the corporate network across a building or campus setting.

The IEEE 802.11 standard is actually only the earliest standard, allowing 1-2 Mbps of bandwidth. Amendments have been made to the original standard to optimize bandwidth or to better specify components in order to ensure improved security or compatibility.
Table 3-3: Variants of 802.11 Standard [21].

<table>
<thead>
<tr>
<th>802.11 Variants</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>802.11a</strong></td>
<td>The 802.11a standard (called WiFi 5) allows higher bandwidth (54 Mbps maximum throughput, 30 Mbps in practice). The 802.11a standard provides 8 radio channels in the 5 GHz frequency band.</td>
</tr>
<tr>
<td><strong>802.11b</strong></td>
<td>The 802.11b standard is currently the most widely used one. It offers a maximum throughput of 11 Mbps (6 Mbps in practice) and a reach of up to 300 meters in an open environment. It uses the 2.4 GHz frequency range, with 3 radio channels available.</td>
</tr>
<tr>
<td><strong>802.11g</strong></td>
<td>The 802.11g standard offers high bandwidth (54 Mbps maximum throughput, 30 Mbps in practice) on the 2.4 GHz frequency range. The 802.11g standard is backwards-compatible with the 802.11b standard, meaning that devices that support the 802.11g standard can also work with 802.11b.</td>
</tr>
<tr>
<td><strong>802.11h</strong></td>
<td>The 802.11h standard is intended to bring together the 802.11 standard and the European standard while conforming to European regulations related to frequency use and energy efficiency.</td>
</tr>
<tr>
<td><strong>802.11n</strong></td>
<td>IEEE 802.11n-2009 is an amendment to the IEEE 802.11-2007 wireless networking standard to improve network throughput over the two previous standards—802.11a and 802.11g—with a significant increase in the maximum raw data rate from 54 Mbps to 600 Mbps along with low power consumption with a range of about 100 feet which makes it the perfect candidate for a home area network in Smart Grid.</td>
</tr>
</tbody>
</table>

The next section in this chapter we will delve into the details of the 802.11 standard architecture.
3.2.2 IEEE 802.11 Architecture

IEEE 802 focuses mainly on the lowest two layers of the OSI model because it involves the physical and data link components. These two layers allows separation of concerns thus allowing a single data protocol to be used with several different RF transmission techniques. The data link layer within 802.11 consists of two sublayers: Logical Link Control (LLC) and Media Access Control (MAC). The MAC layer is responsible for setting the rules for sending and receiving data whereas the physical layer is responsible for the transmission and reception of the data. 802.2 specify the link layer and logic link control [LLC] which could be used by any LAN technology.

The IEEE 802.11 standard is broken into two main layers: the MAC or Media Access Control layer and the PHY or Physical Layer.
3.2.2.1 802.11 Physical Layer

IEEE 802.11 has a physical layer which has two physical medium components as shown in figure 3-21 [23]. They are

Physical Layer Convergence Procedure [PCLP]: It is responsible for communicate to MAC via primitives.

Physical Medium Dependent [PMD]: It is responsible for

- Providing actual transmission and reception of Physical Layer entities via wireless medium.
• Providing modulation and demodulation of the transmission frames.

Figure 3-21: IEEE 802.11 Physical layer components [23].

The physical layers are based on the radio technology and different spread spectrum techniques used. Spread-spectrum technique is a method by which a signal generated in a particular bandwidth is deliberately spread in the frequency domain, resulting in a signal with a wider bandwidth. This technique increases resistance to natural interference and jamming.

- Frequency hopping spread spectrum (FHSS): In this technique the transmitter constantly changes frequency within an assigned range, remaining only a short time on each frequency visited. The receiver must be set to the same hopping code and must listen to the incoming signal at the right time and correct frequency in order to properly receive the signal from the transmitter. This means that both the receiver and the transmitter need to know the pattern beforehand. This can be managed by having a pseudo random generation sequence known to both the
receiver and the transmitter. US Federal Communications Commission (FCC) rules require that, in the most-used bands, the hop sequence using channels spaced at 1 MHz intervals must cover at least 75 channels in the assigned band and not remain on any single channel for longer than 400 milliseconds in any 30-second period [23].

- Direct sequence spread spectrum (DSSS): In this technique the transmitted signal takes up more bandwidth than the information signal that is being modulated. Instead of sending that data as a "narrow band" signal, the DSSS generates a pseudo random code word for every bit in that packet and then combines these code words with the packet by multiplying them together. The pseudo random code words can be 15, 63 or 127 bits. The other 1 bit is the actual data. These code words spread the "narrow" data being sent across a much wider bandwidth than would normally be required. The result is a signal with lower power density, stretched across a wide bandwidth waiting for a receiver to find it. At the DSSS receiver, the same spreading code is reapplied to the spread received power signal once it is found and the wideband signal is narrowed. The data is retrieved intact because the spreading process is independent of the data and when the spreading is cancelled; the data is left in its original state. If there is an interference jammer in the same band, it will be spread out during the de-spreading. As a result, the jammer's impact is greatly reduced. This is the way that the direct-sequence spread-spectrum (DSSS) radio fights interference.
Orthogonal frequency division multiplexing (OFDM): This technique involves splitting the input data into several parallel data streams, modulating each stream onto a separate carrier frequency. At the receivers end all the sub carriers are demodulated and then recombined to form a replica of the original.

Figure 3-22: Major Components of 802.11 [23].

Figure 3-22 [23] shows the major design components in the IEEE 802.11 architecture which are explained below. They are

- **Station**: It is the component that connects to the wireless medium.

- **Basic Service Set (BSS)**: A BSS is a set of stations that communicate with one another. A BSS does not generally refer to a particular area, due to the uncertainties of electromagnetic propagation. When all of the stations in the BSS
are mobile stations and there is no connection to a wired network, the BSS is called independent BSS (IBSS). When a BSS includes an access point (AP), the BSS is called infrastructure BSS. When there is an AP, if one mobile station in the BSS must communicate with another mobile station, the communication is sent first to the AP and then from the AP to the other mobile station.

- Extended Service Set (ESS): An ESS is a set of infrastructure BSSs, where the APs communicate among themselves to forward traffic from one BSS to another and to facilitate the movement of mobile stations from one BSS to another. The APs perform this communication via an abstract medium called the distribution system (DS).

Wireless Medium: It is used to transfer frames between multiple stations and between a station and an access point (AP).

Access Point (AP): It is a device that allows wireless devices to connect to a wired network.

Distribution System (DS): The distribution system is the mechanism by which one AP communicates with another to exchange frames.

The Extended Service Set (ESS) shown in Figure 3-23 [24] consists of a two of overlapping BSSs (each containing an AP) connected together by means of a Distribution System (DS). Although the DS could be any type of network, it is mostly an Ethernet LAN. This design allows mobile nodes to roam between APs, thereby providing seamless campus-wide coverage.
3.2.2.2 MAC Layer

The MAC frame exchange protocol consists of two frames, a data frame sent from the source to the destination and an acknowledgment from the destination that the frame was received correctly. If the source does not get acknowledgement, it tries to transmit according to the basic access mechanism which is CSMA/CA described in the previous sub chapter. This reduces the inherent error rate of the medium, at the expense of additional bandwidth consumption without needing higher layer protocols. Since higher
layer timeouts are often measured in seconds, it is much more efficient to deal with this issue at the MAC layer.

3.2.2.2.1 The Hidden Node Problem

The underlying assumption is that every station can detect transmissions from all other stations. This is not always the case. In figure 3-24 [25], B is within range of the A, but C is not. C would not be able to detect transmissions from A, and the probability of collision is greatly increased. This is known as the Hidden Node. Nodes A and C are unreachable to each other due to their transmission ranges. Also, if both nodes transmit at the same time to B, their frames could be corrupted. This is because wireless communication is half-duplex, which means that transmitting and receiving does not take place simultaneously. IEEE 802.11 MAC frame exchange protocol addresses this problem by adding two additional frames. The two frames are a request to send (RTS) frame and a clear to send (CTS) frame in conjunction with the CSMA/CA scheme.
In Figure 3-25 [25], Source i.e. node A sends RTS and destination i.e. B replies with CTS. The node C is not in the range of a RTS but is in the range of CTS frame sent from node B. Once node A receives CTS it transmits the data frame and waits for an acknowledgement from node B. Since the acknowledgement is in the range of both A and C, it is a clear signal to C that it can send RTS frame. This way a collision is avoided. Nodes that are in range of RTS or CTS suspend transmission for a specified time indicated in the RTS/CTS frames. Stations that hear a CTS suspend transmission until they hear acknowledgement. Any failure in the frame exchange protocol causes the frame to be retransmitted. This is treated as a collision, and the rules for scheduling the retransmission are described in the basic access mechanism which is CSMA/CA. There are retry counters and timers to limit the lifetime of a frame so that the MAC is not
monopolized attempting to deliver a single frame. The RTS/CTS mechanism can be disabled in cases where

- Low demand for bandwidth or not much contention for the channel
- The stations are concentrated in an area where the transmission of every station is heard by all other stations.

Figure 3-25: RTS and CTS address the Hidden Node Problem [25].

3.2.2.3 802.11 Framing

Framing in wireless cannot be as simple as in case of wired as it involves several management features. There are three types of frames namely:

- Data Frames: It is used for data transmission
Control Frames: It is used to control access to the wireless medium such as RTS, CTS, and ACK.

Management Frames: It is used to exchange management information such as beacon frames which is used to identify a BSS.

3.2.2.4 802.11 Security Specification

Security is one of the major concerns when deploying a Wireless LAN. IEEE 802.11 specifies Wired Equivalent Privacy (WEP) for encryption and authentication. WEP has two main parts. The first being the Authentication part the second being the Encryption part. The goals of WEP are:

- Access control: This is achieved by preventing unauthorized users from gaining access as they do not have the correct WEP key
- Privacy: This is achieved by using the WEP key to encrypt the WLAN data streams and only those with the correct WEP key can decrypt them.

Two methods of authentication can be used with WEP: Open System authentication and Shared Key authentication.

Open System authentication: The WLAN client need not provide its credentials to the Access Point during authentication. This means that any system can authenticate itself with the Access Point and then attempt to associate. This is possible even if the system does not have the appropriate WEP key. In effect, no authentication occurs. After the authentication and association, WEP key is used for encrypting the data frames. At this
point if the client does not have the correct WEP key it cannot transmit or receive data. This is because the system is encrypting the data frames with the wrong WEP key and the access point cannot make sense of the data being decrypted with the right WEP key.

Shared Key authentication: The WEP key is used in the authentication process. A four-way challenge-response handshake is used:

- The client station sends an authentication request to the Access Point.
- The Access Point sends back a clear-text challenge.
- The client has to encrypt the challenge text using the configured WEP key, and send it back in another authentication request.
- The Access Point decrypts the material, and compares it with the clear-text it had sent. The Access Point sends back a positive or negative response depending on the success of this comparison.

Figure 3-26: WEP Shared Key Authentication [26].
In shared key authentication, both the unencrypted challenge and the encrypted challenge can be monitored. This leaves the access point open to attack from an adversary who calculates the WEP key by comparing the unencrypted and encrypted text strings. Because of this weakness, shared key authentication is less secure than open authentication.

After the authentication process is the association process which is the mechanism through which IEEE 802.11 provides transparent mobility to stations. Association may only be accomplished after a successful authentication has been completed. When a mobile station requests to be connected to the WLAN, it sends an association request to an AP. The association request includes information on the capabilities of the station, such as the data rates it supports, its contention-free capabilities, its support of WEP, and any request for contention-free services. The AP responds to the mobile station with an association response which includes a status indication. The status indication provides the mobile station with the success or failure of the association request. Once a station is associated, the AP is responsible for forwarding data frames from the mobile station toward the destination.

After the authentication and association, the pre-shared WEP key is also used for encrypting the data frames using RC4. This protects privacy and ensures confidentiality of data, thus fulfilling both the goals of WEP stated above.
4.1 Z-Wave

4.1.1 Introduction

The rising interest in smart grid is a major opportunity to technologies originally developed for home or industrial automation, of which Z-Wave is one of them. The Z-Wave Alliance was founded in 2005 by Zensys, Leviton, Intermatic, Wayne Dalton, Danfoss, CISCO, Intel and UEI. The Z-Wave Alliance is a consortium of manufacturers who build products based on Z-Wave [28]. Z-Wave is a proprietary wireless protocol designed specifically for the residential control and automation market. Conceptually, the intention of Z-Wave is to provide a simple yet reliable method to wirelessly control lights and appliances in a home. Z-Wave protocol was introduced by the small Danish company Zensys. Z-Wave works in industrial, scientific, and medical (ISM) band on the single frequency using frequency-shift keying (FSK) radio [28]. Z-Wave operates at 908MHz (U.S.) and 860MHz (Europe) in unlicensed ISM bands. Each Z-Wave network includes up to 232 nodes and consists of two sets of nodes: controllers and slave devices. Nodes may be configured to retransmit the message in order to guarantee connectivity in multipath environment of residential house. Average communication distance between two nodes is 100 feet, and with message ability to hop up to four times between nodes, it gives enough coverage for most residential houses. About 350 devices from 170
manufacturers now support Z-Wave, a wireless mesh technology that allows home devices such as lighting, appliances, entertainment centers and security systems to interoperable [28].

This chapter gives a brief overview of the following layers:

• The MAC layer
• The Transfer Layer
• The Routing Layer
• The Frame Layer

It also describes the Z-Wave Radio Frequency Protocol that is used to communicate between the control node(s) and the slave nodes in a Z-Wave network.

4.1.2 Z-Wave Protocol Architecture

Z-Wave protocol is a low bandwidth half duplex protocol. A half duplex protocol means that two parties can communicate with each other in both directions, but only one direction at a time. It is designed for reliable wireless communication in a low cost control network. It is used to communicate short control messages in a reliable manner from a control unit to one or more nodes [27]. The control unit will be explained in more detail in the next section. It is not designed to transfer large amounts of data or any data that is critical in nature.

The protocol consists of 4 layers as shown in Figure 4-1 [27]:

The MAC layer: It controls the RF Media.
The Transfer Layer: It controls the transmitting and receiving of frames.

The Routing Layer: It controls the routing of frames in the network.

The Application Layer: It controls the payload in the transmitted and received frame.

Controller and Slave nodes

The Z-Wave protocol consists of 2 basic kinds of devices; controlling devices and slave nodes. The nodes that initiate control commands and sends out commands to other nodes are the controlling devices. The nodes that reply and execute the commands are the slave nodes. Slave nodes can communicate with other nodes as well as forward messages from the controller to other slave nodes. This makes it possible for controllers to communicate with nodes out of direct reach of the controller.

The various devices of a Z-Wave network shown in figure 4-2 [27] are discussed below.
4.1.2.1 Controllers

A controller is a Z-Wave device that has a full routing table and is thus able to communicate with all nodes in the Z-Wave network [27]. When a controller enters the Z-Wave network makes a difference on the functionality available to the controller. If the controller is used to create a Z-Wave network, it automatically becomes the primary controller. The primary controller is the “master” controller in the Z-Wave network and there can be only one in each network [27]. The capability to include or exclude nodes in the network rests with the primary controller. This makes it possible for the primary controller to have the latest topology at all times. Other controllers can be added to the
network as well. These controllers become the secondary controllers, but they do not have the capability to include or exclude nodes from a network.

4.1.2.1.1 Portable Controller
A portable controller is a controller that can change positions physically in the Z-Wave network. It is designed to use various mechanisms to estimate the current location and then calculate the fastest route through the network. An example of a portable controller could be a remote control [27].

4.1.2.1.2 Static Controller
A static controller is also a controller, but one that cannot change positions in the network. It also has to be powered up all the time. The advantage of the static controller is that it does not have to have to calculate its position with relation to the network since it is always constant. It also receives unsolicited status messages from Routing slave nodes. Typically, a static controller will be a secondary controller in the network. An example of a static controller could be an Internet gateway that monitors a Z-Wave system [27].

4.1.2.1.3 Static Update Controller
A Static Update Controller (SUC) is also a controller which is optional in a Z-Wave network. As its name suggests, it is static which means that its position remains constant.
The main functionality is to distribute network topology updates. The SUC receives notifications from the primary controller regarding network topology updates and is capable of sending such updates to other controllers and routing slaves upon request. The application running in a primary controller may request a static controller to become a SUC. Like the primary controller, there can be only one SUC in a Z-Wave network.

4.1.2.1.4 SUC ID Server

A Z-Wave network can also have a SUC with enabled node ID server functionality (SIS), but it is not a necessity. The SIS can be used to enable other controllers to include or exclude nodes from the network on its behalf. The SIS is primary controller in the network and as such always has the latest update of the network topology. The controllers that have this functionality enabled become inclusion controllers since they have the capability to include or exclude nodes in the network on behalf of the SIS. The inclusion controller cannot be classified as a primary controller since it does not have the latest network topology at all times. The network topology is updated only when it requests a network update from the SIS or the last time when a node was included.

4.1.2.1.5 Installer Controller

An Installer controller is a portable controller that has additional functionality that enables it to do more sophisticated network management and network quality testing than
other controllers. An example of an installer controller could be an installation tool used by an installer to install a Z-Wave network at a customer site [27].

4.1.2.1.6 Bridge Controller

A bridge controller is a static controller that incorporates additional functionality or in other words is an extended static controller. The bridge controller functionality can be used to implement controllers that have been targeted for bridging between Z-Wave networks and other networks. The bridge controller stores information about nodes in the Z-Wave network. In addition it can control up to 128 virtual slave nodes. A virtual slave node is nothing but a node that resides on another network type. An example of a bridge controller could be a bridge between a Universal Plug and Play (UPnP) network and a Z-Wave network to link broadband and narrowband devices together in a home entertainment application [27].

4.1.2.2 Slaves

Slave nodes as mentioned before are nodes in a Z-Wave network that receives commands and performs an action based on the command. Slave nodes do not have the capability to send information directly to other slaves or controllers unless requested to do so in a command. An example of a slave node could be a light dimmer [27].
4.1.2.2.1 Routing Slave

Routing slaves have the same overall functionality as a slave. One major difference between a routing slave and a slave node is that a routing slave can send unsolicited messages to other nodes in the network. A number of static routes are stored for use when sending unsolicited messages to a limited number of nodes. An example of a routing slave node could be a thermostat or a Passive Infra Red (PIR) movement sensor [27].

4.1.2.2 Enhanced Slave

Enhanced slaves are slave nodes have the same functionality as routing slaves and are handled the same way in the network. The only difference is that enhanced slaves have a real time clock and an Electronically Erasable Programmable read only memory (EEPROM) for storing application data. An example of an enhanced slave node could be a weather station [27].

4.1.2.3 Home ID and Node ID

Home ID is a unique identifier used by the Z-Wave protocol to separate networks from each other. Home ID is a 32 bit unique identifier which is pre programmed in all controller devices. The slave nodes in a Z-Wave network will initially have a home ID with a zero value and are assigned a home ID by a controller in order to communicate with the network. Controllers in a network exchange home ID’s so that more than one controller in the network can control slave nodes. Individual nodes in the network are
addressed using node ID’s. Node ID’s are unique only within a network defined by a unique home ID’s. A node ID is an 8 bit value. Node ID’s too are assigned to slave nodes by a controller.

4.1.2.4 MAC Layer

The radio frequency medium is controlled by the Z-Wave MAC layer. The data stream is Manchester coded and consists of a preamble, start of frame (SOF), frame data and an end of frame (EOF) symbol. The frame data is the part of the frame that is passed on to the transport layer. The data is sent in little endian format which means that the most significant bit is transmitted first and is transmitted in blocks of 8 bits. The MAC layer is independent of the RF media, frequency and modulation method. However, the MAC layer requires access to the frame data when received or to the whole signal in binary form either as a decoded bit stream or to the Manchester coded bit stream.

4.1.2.4.1 Collision Avoidance

The MAC layer employs a collision avoidance mechanism to prevent other nodes from starting to send data while other nodes are transmitting. The collision avoidance is achieved by letting nodes be in receiving mode when they are not transmitting. The collision avoidance is active on all types of nodes when they have the radio activated. The transmission of the frame is delayed a random number of milliseconds when the media is detected as busy. This way collision is avoided.
4.1.2.5 Transfer Layer

The Z-Wave transfer layer controls the transfer of data between two nodes including retransmission, checksum check and acknowledgements. The Z-Wave transfer layer contains 4 basic frame formats used for transferring commands in the network.

4.1.2.5.1 Frame Layout

All 4 frame types use the frame layout shown in Figure 4-3 [27].

![Figure 4-3: Z-Wave basic frame format](image)

Figure 4-3: Z-Wave basic frame format [27].
The basic frame format used by the following four frame types.

4.1.2.5.1.1 Singlecast Frame Type

When frames are transmitted from one node to another they are called Singlecast frames. The frame is acknowledged so as to notify the transmitter that the frame has been received. A singlecast transmission is shown in Figure 4-4 [27].

![Singlecast Frame Transfer](image)

Figure 4-4: Singlecast Frame Transfer [27].

In Figure 4-4 [27], the ‘Node EFh’ is the transmitter and ‘Node 01h’ is the receiver. If the singlecast frame or the transfer acknowledgement frame from the transmitter is lost, the singlecast frame is retransmitted. In order to avoid potential collisions with parallel systems the retransmissions are delayed with a random delay. The singlecast frame can optionally be used without acknowledgement in a system where reliable communication isn’t required.
4.1.2.5.1.2 Transfer Acknowledge Frame Type

The transfer acknowledgement is a Z-Wave singlecast frame sent from the receiver to acknowledge the reception of the sent frame from the transmitter. The size of the data section is zero in the acknowledgement frame.

4.1.2.5.1.3 Multicast Frame Type

Multicast frames are transmitted from a single node to a number of nodes ranging from 1 to 232 nodes. This frame type doesn’t support acknowledgement. In Figure 4-5 [27], ‘Node EFh’ is the transmitter and nodes ‘Node1h’, ‘Node02h’, ‘Node03h’, and ‘Node04h’ are the receiver nodes. A multicast frame doesn’t get acknowledged so this type of frame isn’t be used for reliable communication. If reliable communication is needed a multicast must be followed by a singlecast frame to each destination node or use of only singlecast frames.

Figure 4-5: Multicast Frame Transfer [27]
4.1.2.5.1.2 Broadcast Frame Type

Broadcast frames are received by all nodes in a network, and just like the multicast frame, it is not acknowledged by any nodes. Figure 4-6 [27] shows data being broadcast from ‘Node EFh’ to all other nodes in the network. A broadcast frame doesn’t get acknowledged so this type of frame isn’t used for reliable transfer. For reliable communication a broadcast must be followed by a singlecast frame to each destination node.

![Figure 4-6: Broadcast Frame Transfer [27]](image-url)
4.1.2.6 Routing Layer

The routing of frames from one node to another is controlled by the Z-Wave routing layer. Both controllers and slaves can participate in routing of frames. The layer is responsible for both ensuring that the frame is repeated from node to node. The routing layer is also responsible for scanning the network topology and maintaining a routing table in the controller.

4.1.2.6.1 Frame Layout

The Z-Wave routing layer has 2 kinds of frames that are used when repeating of frames is necessary.

4.1.2.6.1.1 Routed Singlecast Frame Type

The Z-Wave routed singlecast is a one-node destination frame with acknowledgement that contains repeater information. The frame is repeated from one repeater to another until it reaches its destination.

4.1.2.6.1.2 Routed Acknowledge Frame Type

The Z-Wave route acknowledge is a routed singlecast frame without payload that is used to tell the controller that the routed singlecast has reached its destination.
4.1.2.6.2 Routing Table

The routing table is where a controller keeps the information from the nodes about the network topology. The table is a bit field table where all information about what nodes that can see each other is kept.

Route to Node

Finding the route to a node is a difficult task because a portable controller is defined as a device that will be moved around a lot (e.g. a remote control) Therefore a portable controller will always try to reach a node without routing and if that fails the portable controller will use several techniques to find the best route to the node. Figure 4-8 [29] illustrates a network topology and the resulting routing table. The routing table is build by the primary controller based on information it receives from all the nodes in the network, at installation time, about each nodes range.

Figure 4-7: Routed Singlecast and Acknowledgement Frame Type [27]
4.1.2.7 Application Layer

The Z-Wave application layer is responsible for decoding and executing commands in a Z-Wave network. The only part of the application layer that is described in this overview is the assignment of Home ID’s and Node ID’s and the replication of controllers. The rest of the application layer is implementation specific, and can be different from one implementation to another.

4.1.2.7.1 Frame Layout

The frame format used in the Z-Wave application layer is described in this section.

- Application command:

The application command specifies the specific command or action within the Application command class. In figure 4-9 [27], the following are shown:

---

Figure 4-8: Network topology and routing table [29].
Frame Header: Determines the frame type such as a singlecast, multicast or broadcast.

Application Command Class: Contains the application command which specifies an action or actions.

- Command Classes: Is a collection of functionally related commands.
- Command Parameters: Contains parameters for the specific command.

A device can have several functions and therefore support one or more Command Classes. Most of the Command Classes contain SET, GET, and REPORT command structure. (Command SET allows modification of the data record on the remote node. GET is a request to obtain a value of the data record, and REPORT is a response to a GET request.) To ensure device interoperability, all commands that belong to a particular Command Class must be implemented if the device supports that Command Class.
The figure 4-10 [27] shows the various address bytes reserved for both the Z-Wave protocol and Z-Wave application in the command class.

Currently about 50 Command Classes are defined in Z-Wave [27]. It includes light control, binary and multilevel sensors, thermostat, garage control, etc. To communicate
that the command's classes are supported by a particular device, Z-Wave uses a node
information frames exchange.

- Command parameter 1-x:
The command parameters contain any parameters associated with the specified
command. The number of parameters depends on the command. All frame types except
acknowledge can contain an application command.

4.1.2.7.2 Node information
Because a controller in a Z-Wave network should be able to control many different kinds
of nodes, it is necessary to have a frame that describes the capabilities of a node. Some of
the capabilities will be protocol related and some will be application specific. All nodes
will automatically send out their node information when the action button on the node is
pressed. A controller can also get the node information from a node by requesting it with
a “get node information” frame.

4.1.2.7.2.1 Node Information Frame Flow
The node information frame is send out by a node each time its action button is pressed.
The frame is sent out as a broadcast to any controller/node that is interested in the
information. A controller can request the node information from a node by sending a get
node information frame to it.
In Figure 4-11, the following steps occur when the controller requests node information from a node.

1) The controller requests node information from ‘Node 1’.

2) The node sends an acknowledgement to the controller after receiving the request.

3) The node ‘Node 1’ then sends its node information to the controller.

4) Upon receiving the node information, the controller sends an acknowledgement.

Figure 4-11: Controller requesting Node information [27].

4.1.2.8 Z-Wave Security Specification

The original version of Z-Wave which was implemented on its 100 series chips used triple DES (Data Encryption Standard) encryption scheme with a 56-bit key. A survey was then conducted to see how many customers were using the security services and found that no one was using it [30]. This led to security services being removed in the 200 series.
Figure 4-12 [30] is a comparison of ZigBee and Z-Wave. Although the figure seems to suggest that Z-Wave has optional encryption software, that is only true for the original Z-Wave 100 series chips and not to the current 200 series chips being sold in the market. To counter the problem of security or the lack of it, Z-Wave has a special procedure for the inclusion of new devices in a network. During initial device set-up, the transmissions are at low power so that the signal cannot be detected some distance away by a hacker. Also, the buttons on both the controller and the new device must be pressed simultaneously. In fact, the distance between the primary controller and the new device has to be less than a meter apart. Once the device is included in the network it can be placed anywhere within the range of the network. This still does not nullify the threat of listening in on messages being communicated since there is no encryption scheme.

<table>
<thead>
<tr>
<th></th>
<th>Z-Wave</th>
<th>ZigBee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>868MHz *</td>
<td>2.4GHz</td>
</tr>
<tr>
<td>Data rate</td>
<td>20 kbit/s</td>
<td>250 kbit/s</td>
</tr>
<tr>
<td>Encryption</td>
<td>optional software</td>
<td>AES 128 bit hardware</td>
</tr>
<tr>
<td>Latency</td>
<td>~1000 milliseconds</td>
<td>50-100 milliseconds</td>
</tr>
</tbody>
</table>

*868MHz in Europe and 906MHz in the US

Figure 4-12: Comparison of Z-Wave and ZigBee [30].
4.2 ZigBee

4.2.1 Introduction

ZigBee is a protocol specification and industry standard for a type of wireless communications technology generically known as Low-Rate Wireless Personal Area Networks (LR-WPAN) [32]. The main characteristic of LR-WPAN technology is that it is low cost, low-power consumption and the devices self-organize into a short-range wireless communication network. The network can be a simple-hop star topology or a more complex multi-hop mesh network. Both LR-WPAN and ZigBee are popular because of the above characteristics. The ZigBee specification provides a standardized set of protocols, services, and interfaces for vendors to create LR-WPAN hardware platforms and software applications that will enable customers to deploy complete, interoperable low-power mesh networking systems for monitoring and control [32].

4.2.2 ZigBee Architecture

As mentioned in the introduction, ZigBee is a wireless networking technology standard and is characterized by short-range, low-power consumption, low-data-rate and low-cost. The features of ZigBee networks are self-organization, interoperable application profiles such as SEP (Smart Energy Profile) 1.0 and 2.0 as well as security based on the Advanced Encryption Standard (AES). ZigBee is built upon the lower layers of the IEEE 802.15.4 LR-WPAN standard. The 802.15.4 standard defines the lower-level Physical (PHY) and Media Access Control (MAC) layers while the ZigBee standard defines the
higher-level Network and Application layers as well as the security services. In terms of
general functionality, the Physical Layer provides the basic radio communication
capabilities, the MAC Layer provides reliable single-hop transmission, the Network
Layer provides routing and multi-hop transmission for creating more complex topologies,
the Application Layer provides device and network management functions as well as
message formats, and the Security Services Provider establishes the trust infrastructure of
the network and provides essential security services such as cryptographic key
management and admission control for nodes joining a network [32]. We will be
discussing the layers mentioned above as well the security services. The Figure 4-13 [31]
is a representation of the Zigbee Stack Architecture which is made up of sets of blocks
called layers. Services are performed by each layer for the layer above it. Each layer
exposes an interface to the upper layer through an access point called a Service Access
Point (SAP). Typically, each SAP supports several service primitives to perform the
required functions.
Figure 4-13: Outline of the ZigBee Stack Architecture [31].

The above architecture is based on the Open System Interconnection (OSI) standard seven-layer model. The physical (PHY) layer and the Medium Access Control (MAC) sub-layer are defined by the IEEE 802.15.4-2003 standard. The other layers built on these two layers by the Zigbee Alliance are the Network (NWK) layer and the Application (APL) layer framework. The APL layer is comprised of a Support Sub-layer (APS) and the Zigbee Device Objects (ZDO) along with the manufacturer defined Application objects.
The IEEE 802.15.4 MAC sub-layer uses a Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) mechanism to control access to the radio channel. It is also responsible for reliable transmission of beacon frames and synchronization.

The NWK layer is responsible for applying security for the frames, routing frames to the intended destination, discovering new routes as well as maintaining routes between various devices, storing of neighbor node information, etc.

The APS sub-layer is responsible for maintaining tables for binding and forwarding messages between bound devices. This layer is also responsible for mapping 64 bit IEEE addresses to 16 bit NWK addresses and vice versa.

The ZDO is responsible for defining roles of various devices in the network. For example, defining the role of the Zigbee coordinator or and end node. It would also be responsible for creating and maintaining secure relationships between devices, discovering other devices in the network and the role those devices might play within the network.

4.2.2.1 Application Layer

The application layer consists of the Application framework as well the ZigBee Device Objects (ZDO).
4.2.2.1.1 Application Framework

The application framework is in essence the environment in which Zigbee devices have application objects hosted on them. The application objects receive and transmit data through the APSDE-SAP. The following functions are performed by the application objects:

- Control and management of the protocol layers in the Zigbee device. [31]
- Initiation of standard network functions. [31]

The various data services provided by APSDE-SAP include primitives such as request, response, confirm and indication for data transfer.

- The request primitive: It is used for data transfer between peer application objects.
- The response primitive: It is used to either accept or refuse a request.
- The confirm primitive: It is used to report on the result of a request primitive call.
- The indication primitive: It is used to indicate the transfer of data to the destination object entity from the APS. [31]

Up to 240 distinct application objects can be defined, along with two extra endpoints for APSDE-SAP usage. Endpoint 0 is reserved for the data interface to the ZDO and endpoint 255 is reserved for the data interface to broadcast data to all application objects. The other endpoints 241-254 are reserved for future use.
4.2.2.1.2 Zigbee Device Objects

Zigbee Device Objects provides an interface between the Application objects and the APS. The ZDO is located between the application framework and the APS Sub-Layer.

The ZDO is responsible for the following:

- Initializing the application support sub-layer (APS), the network layer (NWK), and the Security Service Provider. [31]
- Assembling configuration information from the end applications. It also implements other functionality such as
  - Discovery Management: The IEEE or the NWK address of the requested device is returned when asked for by the application object.
  - Security Management: It is used to either enable or disable the security portion of the system and available for use by the application objects.
  - Binding management: It is used to bind application objects on Zigbee devices.

The ZDO provides a public interface to the application objects in the application framework layer. These interfaces provide the application objects a way to control devices and network functions. The ZDO contains an interface on endpoint 0. It interfaces through the APSME-SAP for control messages and also interfaces through the APSDE-SAP for data.
4.2.2.1.3 Application Support Sub-Layer (APS)

The responsibilities of the Application Support Sub-Layer acts as an interface between the network layer (NWK) and the application layer (APL). This is achieved by providing certain services that are used by both the application objects which is manufacturer specific and the ZDO. As mentioned earlier, the services are provided through access points called Service Access Points. In this case the entities and the service access points respectively are

- APS data entity (APSDE) through the APSDE service access point (APSDE-SAP) [31].
- APS management entity (APSME) through the APSME service access point (APSME-SAP) [31].

4.2.2.1.3.1 Application Support Sub-Layer Data Entity (APSDE)

The APSDE provides service for the transmission of data units between devices that are located on the same network. It is also responsible for filtering messages that are addressed to a group and to make sure that the messages reach only that group. It is also responsible for breaking up the data into smaller data units if the payload file is bigger than allowed limit and then assembling them back as they were. This process is called fragmentation and reassemble of data. It is also responsible for reliable data transport.

The services of APSDE are discussed in detail below:
Generation of the Application level PDU (APDU): The APSDE takes an application protocol data unit (PDU) and adds the appropriate protocol overhead to generate an APS PDU.

Binding: This provides the ability to match two devices together based on their services and their needs. The APSDE transfers a message received from one bound device over to the second device, once two devices are bound.

Group Address Filtering: This is the ability to filter group addressed messages based on whether a certain device is a member of that particular group or not.

Reliable transport: Reliability of transactions can be increased by having end-to-end retries.

Duplicate rejection: Messages sent more than once will be rejected by the receiver.

4.2.2.1.3.2 Application Support Sub-Layer Management Entity (APSME)

The APSME provides services that are more management related such as security services. It also provides services such as binding of devices and maintains group addresses. It keeps track of new group addresses that are added and new group addresses that are added from time to time. It maintains a database or a list of objects that it manages. This database is called APS information base (AIB). It is the AIB that is responsible for mapping between 64 bit IEEE addresses and 16 bit NWK addresses.
In addition, the APSME will provide the following services:

- **AIB Management:** The ability to get and set the device’s AIB attributes.
- **Security:** The ability to set up authentic relationships with other devices by using secure keys.
- **Group Management:** This is the ability to add new devices to a group and to remove devices from a group.

4.2.2.2 Network (NWK) Layer Overview

The network layer ensures the correct operation of the IEEE 802.15.4-2003 MAC sub-layer along with providing a suitable service interface to the application layer. It includes two service entities that provide the necessary functionality to interface with the application layer. The two service entities are the data service and the management service. The NWK layer data entity (NLDE) provides service for the transmission of data via its associated SAP, the NLDE-SAP [31]. The NWK layer management entity (NLME) provides the management service via its associated SAP, the NLME-SAP [31]. To achieve it management tasks, the NLME utilizes the NLDE. It also maintains a database of managed objects known as the network information base (NIB). These two services provide the interface between the application and the MAC sub-layer, via the Medium access control common part sub-layer – service access point (MCPS-SAP) and Medium access control sub-layer management entity – service access point (MLME-SAP) interfaces.
4.2.2.2.1 Network Layer Data Entity (NLDE)

The NLDE provides data service to allow applications to transport application protocol data units (APDU) between two or more devices. The devices between which the data is being transferred must be located on the same network. The NLDE will provide the following services:

- Generation of the Network level PDU (NPDU): The NLDE has the ability to generate an NPDU from an application support sub-layer protocol data unit (PDU) by adding an appropriate protocol header.
- **Topology specific routing:** The NLDE has the ability to transmit an NPDU to an appropriate device. The device could either be the final destination in the communication chain or another device via which the data reaches the destination device.
- **Security:** The ability to ensure both the authenticity and confidentiality of a transmission.

### 4.2.2.2.2 Network Layer Management Entity (NLME)

The NLME provides management service to applications so as to allow them to interact with the ZigBee stack.

The NLME provides the following services:

- **Configure new devices:** The ability to configure the ZigBee stack for operation as and when required. The configuration could either be for a ZigBee coordinator or a device intending to join an existing network.
- **Starting a network:** The ability to establish a new network [31].
- **Joining and leaving a network:** The ability to join or leave a network. It also includes the ability for a ZigBee coordinator or ZigBee router to request that a device leave the network [31].
- **Addressing:** The ability for ZigBee coordinators and routers to assign addresses to devices joining the network [31].
Neighbor discovery: The ability to discover, record, and report information pertaining to a device or its one-hop neighbor.

Route discovery: The ability to discover and record paths in the network, so that messages can be efficiently routed.

4.2.2.3 ZigBee Security Specification

The security architecture of ZigBee is described in this section. Security in ZigBee is based on a number of assumptions which if made false expose weaknesses in the system. The following are the assumptions:

- Security provided by the ZigBee security architecture highly depends on the safekeeping of the symmetric keys which in turn is dependent on the protection mechanisms employed and on the proper implementation of the cryptographic mechanisms and associated security policies involved [31].

- Reliance in the security architecture ultimately reduces to reliance in the secure initialization and installation of keying material and to rely in the secure processing and storage of keying material. Implementations of security protocols, such as key establishment, are assumed to properly execute the complete protocol and do not leave out any steps hereof. Random number generators are assumed to operate as expected.

- Secret keys must not become available outside the device in an unsecured way. A device should not intentionally or involuntarily pass on its keying material to
other devices without the keying material being protected. When the network key is being sent to a pre-configured device intent on joining the network, the network key is protected using the master key which has already been configured during manufacture. The only time a key is not protected is when a device that has not been preconfigured joins the network. In this case, a single key may be sent unprotected, thus resulting in a brief moment of vulnerability.

- Due to the low-cost nature of ad hoc network devices, it is not realistic to assume the availability of tamper resistant hardware. Therefore, physical access to a device may yield access to secret keying material and other privileged information and access to the security software and hardware.

- It is not possible for the most part (with the exception of certification) to verify if different layers of the communication stack are properly implemented. It is assumed that separate applications using the same radio trust each other.

- Lower layers such as APS, NWK, or MAC are fully accessible by any of the applications.

- These assumptions lead to an open trust model for a device. Different layers of the communication stack and all applications running on a single device trust each other.

- The provided security services cryptographically protect the interfaces between different devices only. Within a device, the ZigBee stack uses the same key.
Separation of the interfaces between different stack layers on the same device is
arranged non-cryptographically, via proper design of security service access
points.

4.2.2.3.1 Security Design Choices
The open trust model (as described in Chapter 3) on a device allows re-use of the same
keying material among different layers on the same device. This way security is ensured
on a device-to-device basis rather than between pairs of particular layers on two
communicating devices. This allows a compromised network device to use the network
to transport frames across the network without permission.

The following architectural design choices are observed as follows:

- The principle that “the layer that originates a frame is responsible for initially
  securing it” is established [31]. Example: if a MAC layer frame needs protection,
  MAC layer security shall be used or if a NWK command frame needs protection,
  NWK layer security shall be used [31].

- To protect from theft of service, NWK layer security is used for all frames. There
  are certain exceptions to this rule. For example, frames passed between a router
  and a newly joined device (until the newly joined device receives the Network
  key). Consequently, for a device to transmit its messages across more than one
  hop across the network needs to have joined the network and also have received
  the Network key.
Due to the open trust model, security is based on the reuse of keys by each layer of a device. Reuse of keys helps in reducing storage costs but has negatives as well that will be discussed in Chapter 6.

End-to-end security is achieved by having only source and destination devices have access to their shared key. This limits the trust requirement to those devices whose information is at stake [31]. Additionally, this ensures that routing of messages between devices can be realized independent of trust considerations (thus, facilitating considerable separation of concern) [31].

The security level used by all devices in a given network, and by all layers of a device, will be the same if security is used. This is done to simplify interoperability of devices. To be more specific, the security level indicated in the PIB and NIB will be the same. If a scenario arises wherein an application needs more security for its payload than is provided by a given network, it would form its own separate network with a higher security level. Such application profiles should include policies to handle the following conditions:

- Handle error conditions arising from securing and unsecuring packets.
- Detect and handle loss of key synchronization.
- Expire and periodically update keys, if need be.

Amongst a network of ZigBee devices, security is based on ‘link’ keys and a “network” key. Unicast communication between APL peer entities is secured by means of a 128-bit link key shared by two devices, while broadcast communications are secured by means of
a 128-bit Network key shared amongst all devices in the network [31]. The device the data intends to reach or the destination device is always aware whether a frame is protected with a link or a Network key.

A device obtains link keys either via

- **Key-transport:** The key is transported via the NWK layer using a common “network” key.
- **Key-establishment:** The device initiating a request established a “link” key using a master key that may either be pre-installed during manufacture or installed by a third party device or a trust center.
- **Pre-installation:** It could be during factory installation.

A device obtains a Network key via key-transport or pre-installation. Eventually, security between devices depends on the secure establishment and maintenance of these keys.

In a secured network there are a variety of security services available. The Network key may be used by the MAC, NWK, and APL layers of ZigBee. The link and master keys may be used only by the APS sub-layer.

4.2.2.3.2 ZigBee Security Architecture

ZigBee applications communicate using the IEEE 802.15.4-2003 wireless standard which is discussed in the previous chapter. The Physical (PHY) and Medium Access Control (MAC) layers which are part of the IEEE 802.15.4-2003 wireless standard were discussed. ZigBee adds a Network (NWK) layer and an Application (APL) layer on the
PHY and the MAC layers of IEEE 802.15.4-2003. The PHY layer provides the basic communication capabilities of the physical radio [31]. The MAC layer provides services so as to have reliable, single-hop communication between devices [31]. The ZigBee NWK layer is used to provide routing and multi-hop functions that will be required in order to transfer data across a network having different network topologies such as star, tree, and mesh topologies. The APL layer as previously mentioned includes an Application Support (APS) sub-layer, the ZigBee Device Object (ZDO), and applications [31]. The ZDO controls device management as well as manages security configurations and policies of a device. The APS layer acts as a foundation to service the ZDO and ZigBee applications. It provides services such as establishing and maintaining security relationships.

The architecture includes security mechanisms at three layers of the protocol stack. The MAC, NWK, and APS layers are responsible for the secure transport of their respective frames. The security mechanisms provided by the MAC, NWK and APS layers are described in the following sub-chapters.

4.2.2.3.2.1 MAC Layer Security

ZigBee uses the MAC layer security as specified by the 802.15.4 specification with a little modification to secure a frame originating at the MAC layer. The modification is necessary for one of ZigBee’s security needs which is the ability to protect incoming and outgoing frames using the security levels based on CCM*. CCM* is a minor modification
of CCM (Counter with CBC-MAC (Cipher Block Chaining Message Authentication Code)) specified in 802.15.4 MAC layer specification. CCM* includes all of the features of CCM and furthermore offers encryption-only and integrity-only capabilities. The CCM* mode allows the length of the Authentication field to be zero. This for all intents and purposes disables authenticity as the Authentication field is an empty string. These extra capabilities simplify security by eliminating the need for CTR and CBC-MAC modes. Since ZigBee follows the open trust model, it is important that all layers (MAC, NWK, and APS layers) be able to reuse a common key. The use of CCM* also enables the use of a single key for all CCM* security levels [31]. The MAC layer is responsible for its own security processing, but the upper layers can determine the security level they want to use. For ZigBee, MAC layer frames that require security processing use the security material from the attributes of the MAC Personal area network information base (PIB). Figure 4-15 [31] shows the security fields that may be included in an outgoing frame with security applied at the MAC level.

Figure 4-15: ZigBee Frame with security at the MAC level [31].
4.2.2.3.2.2 NWK Layer Security

Similar to the MAC layer, the NWK layer's frame protection mechanism uses the Advanced Encryption Standard (AES) and CCM*. Management of NWK layer security by Upper layers is done by setting up active and alternate Network keys and by determining which security level to use. NWK layer has a responsibility to route messages over multi-hop links. A part of this responsibility includes the NWK layer broadcasting route request messages as well as processing received route reply messages. Route request messages are simultaneously broadcast to nearby devices and route reply messages originate from nearby devices [31]. The NWK layer shall use the link key to secure outgoing NWK frames, if the appropriate link key is available. If the appropriate link key is not available, in order to secure messages against outsiders the NWK layer uses its active Network key to secure outgoing NWK frames and either its active Network key or an alternate Network key to secure incoming NWK frames [31]. In such scenarios, the frame format explicitly indicates the key to be used to protect the frame; therefore, intended recipients can infer which key to use for processing an incoming frame and also determine if the message is readable by all network devices, rather than just by itself. Figure 4-16 [31] shows an example of the security fields that may be included in a NWK frame.
4.2.2.3.2.3 APL Layer Security

When a frame originating at the APL layer needs to be secured, the APS sub-layer handles security for that frame. The APS layer allows frame security to be based on link keys or the Network key [31]. Figure 4-17 [31] shows an example of the security fields that may be included in an APL frame. The APS layer is also responsible for providing applications and the ZDO with key establishment, key transport, and device management services.
4.2.2.3.3 Security Keys Establishment

The APS sub-layer's key establishment services provide the mechanism by which a ZigBee device may derive a shared secret key otherwise called a link key with another ZigBee device [31]. Key establishment involves two entities, an initiator device and a responder device, and is prefaced by a trust provisioning step [31]. A master key acts a starting point for establishing a link key. Once trust information is provisioned, a key-establishment protocol involves three steps:

- The exchange of transient data.
- The use of this transient data to derive the link key.
- The confirmation that this link key was correctly computed.

In the Symmetric-Key Key Establishment (SKKE) protocol, an initiator device establishes a link key with a responder device using a master key. This master key, for example, may be pre-installed during manufacturing or may be installed by a trust center which could be the initiator, the responder, or a third party device acting as a trust center or may even be based on user-entered data such as a PIN, password, or key. The master keys secrecy and authenticity needs to be maintained in order to maintain a trust foundation.

- Transport Key

This is a service by means of which a device transports a key to another device either securely or unsecurely. The secured transport-key command provides a means to
transport a master, link, or Network key from a key source, usually a trust center, to other devices. The unsecured transport-key command is how a device is loaded with an initial key. This command does not cryptographically protect the key being loaded [31]. In this case, the security of the transported key can be realized by non-cryptographic means, for example, by communicating the command via an out-of-band channel that guarantees secrecy and authenticity [31].

- **Request Key**

  The request-key is a service by means of which a device may request the current Network key, or an end-to-end application master key, from another device such as it trust center.

- **Switch Key**

  The switch-key is a service by means of which a device such as a trust center may inform another device that it should switch to a different active Network key.

4.2.2.3.4 Trust Center Role

The trust center is the device within a network that distributes keys for network and end-to-end application configuration management. There is one and only one trust center in a secure network which would be recognized by all the network members. In high-security, commercial applications, a device may come pre-loaded with the trust center address and initial master key. On the other hand, if the application is not critical, the master key can
be sent via an in-band unsecured key transport. If not pre-loaded, a device’s trust center defaults to the ZigBee coordinator. In low-security, residential applications a device securely communicates with its trust center using the Network key, which can be preconfigured or sent via an in-band unsecured key transport [31]. The functions performed by the trust center are divided into three sub-roles:

- **Trust Manager:** It is responsible for identifying the device(s) that take on the role of its network and configuration manager.
- **Network Manager:** It is responsible for distributing and maintaining the Network key to the devices it manages.
- **Configuration Manager:** It is responsible for binding two applications and enabling end-to-end security between devices it manages (for example, by distributing master keys or link keys) [31].

These three sub-roles are contained within a single device – the trust center.

A device accepts an initial master or Network key originating from its trust center via unsecured key transport. It accepts an initial Network key and updated Network keys only from its trust center (that is, its network manager) and accepts master keys or link keys for the purpose of establishing end-to-end security between two devices only from its trust center (that is, its configuration manager). Apart from the initial master key, additional link and Network keys are accepted if and only if they originate from a device’s trust center via secured key transport.
In this chapter, the focus is on the security issues and vulnerabilities of the protocols or standards discussed in chapter 3 and chapter 4. Wireless networks are more prone to attacks because the communication medium is easily accessible.

5.1 IEEE 802.15.4 Security Vulnerabilities

1) No support for Group Keying [18]

Group keying is not very wieldy in the 802.15.4 standard. If nodes ‘n1’, ‘n2’, ‘n3’, ‘n4’, ‘n5’ wish to communicate with each other using a key ‘k1’ while nodes ‘n6’, ‘n7’ and ‘n8’ wish to communicate using key ‘k2’, this is not possible since each ACL entry can be associated to a single destination address.

2) Network Shared Keying Incompatible with replay protection [18]

Replay attacks are hard to prevent when using a single network-wide shared key. Suppose a node ‘n1’ sends 10 messages encrypted with the shared network key using replay counters from 0 to 9. The next value the receiving node ‘n2’ is expecting a value of 10. If another node sends node ‘n3’ a message encrypted with the same network wide key and a message counter again starting from 0 to node ‘n2’, the message is rejected.

3) Insufficient Integrity Protection [18]

The AES-CTR security suite uses AES encryption but protects the cipher text with a CRC (Cyclic Redundancy Check). It is relatively easy to modify a packet to make sure
that the CRC remains the same for different packets. This way the integrity of the packet is damaged. One wrong assumption to make is that a strong encryption algorithm is enough since decrypting with the wrong key will yield garbage. A strong integrity check is required to protect integrity as well. A weak integrity check can compromise confidentiality as well by tricking the end user into disclosing secrets.

4) Denial of Service [18]

Denial of service attacks can be used on an 802.15.4 network using the AES-CTR suite with replay protection enabled. Example: A sender s and a recipient communicate using a key k. The recipient always expects a counter value with a higher value than the previous packet. An adversary can send a forged packet with a very high key counter and very high frame counter value with the address of the sender s which might not be a valid cipher text. The message will be accepted since there is no access control or message authentication. The recipient will decrypt the packet with the secret key k resulting in an invalid cipher text. However, before passing the garbage payload to the higher layers, the MAC layer will update the high water mark to the high value sent by the attacker. Any legitimate packet sent after this will be rejected since the nonce value will be lesser than the nonce value in packet sent by the adversary.
5.2 IEEE 802.11 Security Vulnerabilities

1) Wireless Sniffing

It is very easy to “listen” to wireless networks. People can travel around the city with a wireless-compatible laptop or smart phones looking for wireless networks. This practice is also called war-driving. Specialized war-driving software allows the locations of open access points to be mapped accurately with the help of a Global Positioning System (GPS) [34].

The risks involved in not properly securing a wireless network are

- Data interception: This is the practice of listening in on data transmissions in the network. Data to and from various users in the network is at risk of being read thus violating confidentiality.
- Cracking: It is the practice of attempting to access a local network or the internet.
- Network Intrusion: Aside from allowing the adversary to access the internet, it also allows the attacker to launch cyber attacks using the unsecured network. In such cases, the business that installed the access point would be held responsible for the attack.
- Denial of Service: Non availability of service is called Denial of Service. The 802.11 standard's network access method is based on the CSMA/CA protocol, which involves waiting until the network is free before transmitting data frames. An attacker may simply keep sending bogus packets to the access point. This
would keep the channel busy thus preventing authentic users from using the service.

2) Evil Twin Attacks

The adversary gathers information about a public access point and then sets up one’s own device to mimic the real access point. By using a broadcast signal stronger than the one generated by the real access point, the adversary can fool users into thinking that his device is a better access point (AP). Any number of software can be installed so as to read the data sent from users connected to his or her device.

3) Inadequate Encryption Standards

Wired equivalent privacy (WEP) is a weak encryption standard. WEP uses the stream cipher RC4 for confidentiality. RC4 is a stream cipher that uses an IV (Initialization Vector), which is transmitted along with the data packet as plain text to prevent replay attacks. But a 24-bit IV is not long enough to ensure this on a busy network. For a 24-bit IV, there is a 50% probability the same IV will repeat after 5000 packets [35].

4) Radio Jamming

Radio waves are sensitive to interference. A signal can easily be jammed by a radio transmission with a frequency close to that used by the wireless network. A simple microwave oven operating at the same frequency could make the network inoperable if used within the range of an access point [34]. This is achieved by inducing noise into the network and thereby reducing the signal to noise ratio of the channel to an unusable range. This is also a Denial of Service (DoS) attack.
5) Peer-to-Peer Connections

Most laptops nowadays come equipped with the 802.11 Wi-Fi wireless networking cards. Laptops themselves can create ad hoc networks if within range of one another. Thus computer-to-computer connections can be set up. If the attacker with a network card configured for ad hoc mode uses the same setting as another user, the attacker could gain unauthorized access to personal files. This type of attack have been occurring more frequently since many companies ship laptops and PCs with the wireless cards set to ad hoc mode by default[36].

5.3 Z-Wave Security Vulnerabilities

1) Eavesdropping

Since there is no encryption used in Z-Wave, all messages are sent in plain text. This makes it susceptible to eavesdropping. An adversary within the range of the network can listen in on the messages being transmitted.

2) Man-in-the-middle Attack

This is a form of active eavesdropping. Since all the messages are sent in plain-text, an adversary may resend the same message by pretending to be the actual device since the address of the sender and the destination is known. For example: By observing activity at a home, the eavesdropper could work out the meaning of packets, for example that a certain number means turn on the washing machine. Then the eavesdropper could rebroadcast the packet, and thereby reproduce the same action.
5.4 ZigBee Security Vulnerabilities

In this section we highlight security concerns that have been found in the Smart Energy Profile 1.0.

1) Forward Security

When a device leaves the network or is forced to leave the network in case it is compromised, the device must not have access to any further communication in the network (forward security). If a compromised device can still access communication in a network, the adversary may abuse the keying material stored on the device. To accomplish this, a proper key revocation and redistribution policy is required. When a device leaves the network for whatever reason, the key is to be deleted and a new one must be sent to all members in the network. This way the device no longer has any access to communication in the network. The Smart Energy Profile 1.0 does not mention anything about Network and Link Key management [37]. Also, a device that leaves the network retains the network key and the Link keys established with other peer devices. This would mean that the device would still be able to listen and/or actively take part in all communications that use the network and Link keys for security. This could allow the compromised device to send bogus routing information called sinkhole attacks.

The ZigBee Specification dictates that the Trust Center must refresh such a key periodically [37]. Since it is not event driven such as upon a device leaving or joining the
network, it gives the adversary a time frame during which the adversary access to communication in the network \cite{37}.

2) Backward Security

When a new device joins the network, it should not be able to access messages that were communicated in the network before it joined. However, the Zigbee specification refreshes the network key periodically. This would allow the new device to access messages that it has no right to access.
Chapter 6
COUNTER MEASURES AND BEST PRACTICES

In this chapter the focus is on counter measures to various attacks discussed in the previous chapter. Also, various best practices are discussed in length.

6.1. 802.15.4 Counter Measures and Best Practices

The following section describes the recommendations for the security of 802.15.4 networks:

1) IV Management Solutions [34]

The best way to overcome this issue is by using a single ACL entry. Using single ACL entry, the sender can send the first message and then send the second message by changing the destination address in the same ACL entry. In addition to this, nonce reuse can be taken care by not separating the nonce state from the key.

2) Flash Memories [23]: The loss of ACL entries during power failure or low powered operation can be fixed by saving and storing the nonce states in flash memories. The problem with this however is that flash memories results in additional cost, power consumption and also is slow and energy inefficient.

3) MAC Address Filtering [23]: This is a basic security mechanism employed to prevent unauthorized nodes from joining the network. The MAC maintains a list of device addresses with which it will communicate. This security mechanism is provided in the
IEEE 802.15.4 standard and is defined in the Access Control List (ACL) mode. This does not prevent against MAC spoofing but should be enabled all the same.

4) Source Node Authentication [23]: Link keys are shared secret keys between FFDs (fully functional devices) and RFDs (reduced functional devices). They are derived from a master key and are a safe way to authenticate the source node.

5) AES Encryption Standards [23]: AES encryption standard should be used to protect data confidentiality.

6.2 IEEE 802.11 Counter Measures and Best Practices

The following section describes the recommendations for the security of 802.11 networks:

1) Media Access Control (MAC) Address Filtering [23]: This allows configuration of wireless access points (APs) with the set of MAC addresses for authorized wireless clients. This is achieved by using access control lists (ACL). While this helps prevent unauthorized access for the most part, it does not prevent an adversary from spoofing MAC addresses.

2) Wi-Fi Protected Access (WPA) [23]: This is an improved encryption algorithm called Temporal Key Integrity Protocol (TKIP) which uses a unique key for every client and also uses longer keys that are rotated at configurable intervals [23]. WPA also includes an encrypted message integrity check field in the packet to prevent capturing, altering and resending data packets. The use of WPA2 is highly desirable as it is more secure than
both WEP and WPA. However, the downside is that some old network cards do not support WPA2.

3) IEEE 802.11w-2009 [23]: The management information is sent in unprotected frames, which cause network disruption by malicious systems that forge disassociation requests that appear to be sent by valid equipment. IEEE 802.11w-2009 is an approved amendment to IEEE 802.11 to increase security of the management frames. The objective of this protocol is to increase the security by providing data confidentiality of management frames and other mechanisms that enable data integrity, data origin authenticity, and replay protection.

4) Make the Wireless Network Invisible

Wireless access points broadcast their presence to wireless-enabled computers. This is desirable in networks that are for the public such as in a railway station. This way customers and traveler’s can use the publicly available internet for free. In other cases such as in businesses or defense broadcasting one’s service set identifier (SSID) is not desirable. This should not be the only security setting since it would create a “security through obscurity” which is not foolproof and easily deceivable. This is also called a closed network [36].

5) Encrypt Network Traffic

All communication between an access point and the end device must be encrypted. This helps protect confidentiality [36].
6) Change Administrator Password

Wireless access points are shipped with default usernames and passwords. This should be changed since the defaults are known and recorded on public sites. Gaining access to such a network would not be very difficult [36].

7) Rename the Wireless Network

Many wireless access point devices have a default name from the manufacturer called SSID. The default names of each manufacturer are known and can be got from hundreds of sites online. Once the wireless network is invisible, renaming the wireless network is essential to prevent unauthorized access [36].

8) Connect using a VPN

VPNs allow employees to connect securely to their network when out of office. Using a virtual private network (VPN) is secure since the connections at the sending and the receiving end are encrypted. This way the data is secure. [36].

9) Disable File Sharing

This is to counter the effect of data being exchanged inadvertently between two peer-to-peer networks. In wireless spaces, file sharing is even more dangerous since there is unknown number of users who could potentially access ones computer. Disabling file sharing in public wireless networks is a good way to nullify the threat of peer-to-peer connections [36].
6.3 Z-Wave Counter Measures and Best Practices

1) Use Standard Encryption Mechanisms
Using an industrial grade security such as Advanced Encryption Standard (AES) would solve problems such as active and passive eavesdropping.

6.4 ZigBee Counter Measures and Best Practices

1) Forward Security Solution
Rekeying and redistribution of the network and Link key during an event as well as periodically is one such solution [37]. This way the compromised device will not have access to communication once it has been forced to leave the network. This would result in more overhead but more security.

2) Backward Security Solution
The same solution proposed in [37] for forward security would work for backward security as well. If the network key is changed every time a device joins a network the backward security problem is solved as well.

3) Discourage AES-CTR Security Suite
AES-CTR which is explained in Chapter 3 is an unauthenticated suite which has major weaknesses as described in the previous chapter. Since AES-CTR is optional, ZigBee would still be standard compliant even if it doesn’t implement this security suite. Also, AES-CTR does not provide sequential freshness as the specification claims [37].
ZigBee Security Best Practice Recommendations

The following are recommended practices that should be considered when implementing a ZigBee LR-WPAN network:

1) Create a lr-wpan security policy and set of procedures to govern the implementation, management and operation of ZigBee Networks [32].

A general LR-WPAN technology security policy should be developed. It can be in high level non-technical language so that the management can understand and implement it. The policy should include the roles and responsibilities of various individuals in the organization so as to ensure safe and secure operation.

2) Protect the ZigBee Network Infrastructure with a Network Key [32].

Ideally all nodes communicating in the network must be forced to use the network key. The routing nodes must validate the ZigBee packets based on the Network Key before forwarding the packets. This way a node without a valid network key will not be able to join or utilize a ZigBee network for transport.

3) Implement address filtering at the MAC layer [32].

Use Access Control List (ACL) to implement address filtering. This way only an authorized node is able to communicate and use the network. This is a low level security mechanism since it doesn’t protect against MAC is discussed in the Chapter 6.1.
4) Utilize the ZigBee encryption security service [32].

The ZigBee standard provides data confidentiality based on AES encryption scheme. This should be enforced and not be an option.

5) Designate a ZigBee Coordinator [32].

The IEEE 802.15.4 protocol defines fully functional devices (FFD) and reduced functionality devices (RFD). Any FFD has the potential to become a ZigBee coordinator. Since many FFDs may exist at the same time in a ZigBee network, any one of them could become a ZigBee coordinator. This type of uncertainty may not be desirable. Therefore a coordinator is designated beforehand to have more control.

6) Designate a backup ZigBee Coordinator if supported [32].

If the dedicated ZigBee coordinator is down, all nodes except one should be configured to be the backup coordinator. This prevents other nodes from establishing a new separate LR-WPAN network on their own.

7) Choose and out-of-band key loading method if possible [32].

The initial generation and loading of cryptographic keys such as the Master key is possible in three ways.

Out-of-band: This method loads the ZigBee device other than a wireless method such as a cable from the trust center host or a trusted device into the ZigBee device.
In-band: This method loads the ZigBee key through normal wireless communication channels.

Factory pre-loaded: In this method the ZigBee key is generated and loaded by the vendor into the ZigBee devices. This is the least secure method since the vendor knows the key values and must convey it to the customer.
Chapter 7

POTENTIAL RESEARCH AREAS

7.1 Security Issues in Smart Energy Profile 2.0

ZigBee Smart Energy Profile (SEP) is an application profile designed to promote interoperability between different devices in a HAN as well as between the utility company and the household devices. Energy efficiency is improved by allowing consumers to choose interoperable products from different manufacturers and thus having the means to manage one’s energy consumption using automation. Having real time information about current energy usage plays a big role in energy consumption since consumers know how much energy is being used at a certain time. It also helps utilities with demand response, load control and pricing. SEP 1.0 specifies the ZigBee 2007 radio communications stack. Version 1.0 provides a core set of functions that smart energy devices may need, such as programmable communicating thermostats, in-home displays, and direct load controllers.

SEP 2.0 is a united effort by the ZigBee Alliance and the HomePlug Power Alliance. It uses an IPV6 stack instead of the ZigBee stack used in SEP 1.0. This makes it incompatible with the previous version. SEP 2.0 Technical Requirements Document (TRD) has been released to the public in March, 2011 along with the Marketing Requirements Document (MRD). The final SEP 2.0 specification document is expected
to be out by December, 2011. Since the stack used is different from the previous versions, the security issues in the new profile could be a potential research topic.

7.2 Erratic Latencies in Wireless Mesh Networks

The advantage of wireless mesh networks is that it is both self-healing and self-organizing. It is self-healing in the sense that if a node is down a message can still reach the destination by re-routing the message using routing algorithms to update the routing table. It is self-organizing in the sense that a new node is automatically detected and incorporated into the network. The disadvantage is that as the size of the network grows, the number of hops taken to reach a destination increases and the throughput decreases due to interference. Any packets that get lost en route get retransmitted creating unpredictable latencies. Reducing the latencies in such events is a possible area of research since both Z-Wave and ZigBee are both mesh networking protocols and are serious contenders as HAN protocols in Smart Grid.

7.3 Security for Routing in Wireless Mesh Networks

There are multiple security threats to wireless mesh networks such as

Worm-Hole: In this attack an adversary connects two distant points in the network using a direct low-latency communication link called as the wormhole link. The wormhole link can be established by a variety of means, e.g., by using a ethernet cable. Once the
wormhole link is established, the adversary captures wireless transmissions on one end, sends them through the wormhole link and replays them at the other end.

Sink-Hole: Here the attacker creates forged packets to imitate a valid node in the mesh network. The packets are attracted by advertizing low cost routes and further attacking by dropping the packets.

Byzantine Attack: Byzantine attack means that attackers may modify the coded packets.

Rushing Attack: Route Request messages (RREQ) are used to discover new routes. By forwarding the RRQ messages quicker than legitimate nodes, the attacker’s nodes and routes are more likely to be discovered than legitimate nodes and routes.

Routing Table Overflow Attack: In this attack an adversary attempts to create routes to non existent nodes. By creating enough routes to non existent nodes, new routes cannot be created.

Resource Consumption Attack: Resource consumption DOS attacks are when network resources are overburdened and cause the rest of the network to slow down.

Location Disclosure Attack: This type of an attack reveals information about the location of the node. It may also reveal information about the structure of the network.

Sleep Deprivation: This type of attack is practical only in mesh networks where battery life is critical. The victim node is flood with fake request messages thus preventing it from entering a sleep mode to conserve battery.

Eavesdropping: This attack involves listening in on messages that are being communicated in the network.
7.4 Wireless Intrusion Detection Limitations

Intrusion Detection systems (IDS) as the name suggests are used to detect intrusions into a system by an adversary. The problem with IDS is that even minor modifications or deviation from normal behavior of the system results in a false positive. The investigation that goes into such occurrences is time consuming. Also there is the possibility of IDS not detecting an intrusion. This is called a false negative. This is a potential area of research.

7.5 802.11 MAC Management Attacks

12 byte addresses are used to identify 802.11 nodes at the MAC layer. Both the sender address and the receiver address is stored in the MAC frame and is determined by the sender. The real problem is that the 802.11 standard does not include any mechanism for verifying the correctness of the sender. This makes it possible for an adversary to spoof other nodes. This vulnerability is taken advantage of during the authentication process which allows clients and access points to explicitly request de-authentication from one another. Since the message itself is not authenticated using any keying material, the attacker may spoof this message, either pretending to be the access point or the client, and send it to the other party. This same type of attack can be implemented in the de-association process although it is a little less efficient attack as there is less work to associate once again.
7.6 Denial of Service Attacks

The above spoofing attacks can be used to launch denial of service attacks as well. By denying a victim node or an AP from association with each other, it results in a denial of service attack.
The project focuses on Home Area Network protocols and standards for Smart Grid. Home Area Networks play an important role in the consumer side and are integral to the existence of Smart Grid. Some of the security requirements for Home Area Networks are access control, confidentiality, integrity and accountability. Some of the other general requirements are low cost, power efficiency and reliability.

This project discusses a few wireless candidate protocols/standards for Home Area Networks in Smart Grid such as IEEE 802.15.4, IEEE 802.11, Z-Wave and ZigBee. Wireless protocols were selected as it is both inconvenient and impractical to have wires connected between all devices in a household. The above mentioned protocols are well suited to most of the specifications mentioned. They are also listed among the standards for Home Area Networks in the NIST Framework and Roadmap for Smart Grid Interoperability Standards document.

In all of the protocols and standards discussed, ZigBee is better suited to the needs of Home Area Networks than the other protocols. ZigBee has the advantage of being low-cost, highly scalable to very large networks and a good battery life. The advantage that both Wi-Fi and Z-Wave have is market penetration where both protocols have a big presence in households across the U.S. The disadvantage of Z-Wave is that it is a
proprietary protocol. Also, the absence of security services is a major disadvantage. An inclusion of the AES standard for enforcing confidentiality is currently being discussed. The research done in this project can be extended to overcome some of the issues mentioned in Chapter 7.
BIBLIOGRAPHY


http://science.howstuffworks.com/environmental/energy/power.htm


http://www.nema.org/gov/energy/smartgrid/whatIsSmartGrid.cfm


Coming Smart Grid”, [Online]. Available:
id.html

“Home networking with IEEE 802.15.4: a developing standard for low-rate wireless
personal area networks”, Communications Magazine, IEEE, Vol.40, Iss.8, Aug 2002
Pages: 70- 77.

“IEEE 802.15.4: a developing standard for low-power low-cost wireless personal area


[16] IEEE, “802.15.4-2003 - IEEE Standard for Local and Metropolitan Area Networks -
Specific Requirements - Part 15.4: Wireless Medium Access Control (MAC) and
Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks
(WPANs)”, [Online] Available:

http://profsite.um.ac.ir/~hyaghmae/ACN/WSNMAC1.pdf

http://wireless.arcada.fi/MOBWI/material/prints/PRINT_ZigBee.html


http://www.eetimes.com/design/communications-design/4025721/Catching-the-Z-Wave/


[31] ZigBee Alliance, “ZIGBEE SPECIFICATION v1.0”, [Online] Available:


