UNIVERSITI PUTRA MALAYSIA

SECURITY IMPROVEMENT OF UNICAST MANAGEMENT FRAMES IN IEEE 802.11 MAC LAYER

MINA MALEKZADEH

FSKTM 2007 14
SECURITY IMPROVEMENT OF UNICAST MANAGEMENT FRAMES IN IEEE 802.11 MAC LAYER

By

MINA MALEKZADEH

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirement for the Degree of Master of Science

August 2007
DEDICATION

To my mother and my father

Who my love to them is never ending

My husband Hadi and my children Zahra and Reza

Who I am nothing without them
SECURITY IMPROVEMENT OF UNICAST MANAGEMENT FRAMES IN IEEE 802.11 MAC LAYER

By

MINA MALEKZADEH

August 2007

Chairman: Associate Professor Abdul Azim Abdul Ghani, PhD

Faculty: Computer Science and Information Technology

Wireless Local Area Network (WLAN) or IEEE 802.11, was formed in 1990 to exchange information by using radio frequency rather than wires. This standard transmits information by three types of frame: data frame, control frame, and management frame.

To provide security for WLANs, different security protocols have been designed such as: wired equivalent privacy (WEP), wifi protected access (WPA), and the strongest one, IEEE 802.11i (WPA2). Unfortunately all of the mentioned protocols provide security only for data frame. Control and management frames are transmitted without any protection even in IEEE 802.11i. The lack of protection on management frames causes an intruder to launch different types of attack on the WLAN such as forgery, session hijacking, denial of service and man-in-the-middle attack, which can lead to expose the whole WLAN.

To address the problem, this thesis proposes and evaluates a new per frame security model which is called Management Frame with Integrity and Authentication (MFIA)
to authenticate transmitted management frames. The proposed model uses a secret key and a new random sequence number (RSN) to secure communication between devices in WLAN and to prevent intruder from exposing the WLAN. The proposed model checks the authentication of a sender and the integrity of the management frames.

The proposed model has been evaluated by quantifying the probability of finding a proper RSN by intruder, probability of different current common attacks on management frames, and also required time for the specified attacks. The results show that MFIA provides a high security level for management frames in all IEEE 802.11 standards. Required times to launch the attacks, show that allocating the specified time by intruder is almost impossible in the proposed model so that makes the mentioned attacks impractical. Results also show the proposed model can prevent a variety of attacks on management frames.
Sebagai memenuhi keperluan untuk Ijazah Master Sains

PENAMBAHBAIKAN KESELAMATAN KERANGKA PENGURUSAN DALAM LAPISAN MAC IEEE 802.11

Oleh

MINA MALEKZADEH

Ogos 2007

Penyelia: Profesor Madya Abdul Azim Abdul Ghani, PhD

Fakulti: Sains Komputer dan Teknologi Maklumat


Untuk menyediakan keselamatan bagi WLAN, protokol keselamatan berbeza telah direka bentuk seperti: wired equivalent privacy (WEP), wifi protected access (WPA), dan yang terkukuh, IEEE 802.11i (WPA2). Malangnya semua protokol yang dinyatakan menyediakan keselamatan hanya untuk kerangka data. Kerangka kawalan dan pengurusan dihantar tanpa sebarang perlindungan walaupun dalam IEEE 802.11i. Kekurangan perlindungan ke atas kerangka pengurusan menyebabkan penceroboh melancarkan pelbagai jenis serangan ke atas WLAN seperti pemalsuan, merampas sesi, penafian perkhidmatan, dan serangan orang-tengah yang mendedahkan keseluruhan WLAN.

Untuk mengatasi masalah ini, tesis ini mencadang dan menilai model keselamatan per kerangka yang dipanggil Management Frame with Integrity and Authentication
(MFIA) untuk mengesah kerangka pengurusan yang dihantar. Model cadangan menggunakan satu kunci rahsia dan nombor jujukan rawak (RSN) untuk melindungi komunikasi diantara peranti dalam WLAN dan menghalang penceroboh daripada mendedahkan WLAN. Model cadangan memeriksa ketulenan penghantar dan integriti kerangka pengurusan.

Model cadangan telah dinilai dengan cara mengkuantitikan keberangkalian untuk mencari RSN yang wajar oleh penceroboh, keberangkalian pelbagai serangan yang biasa ke atas kerangka pengurusan, dan juga masa yang diperlukan untuk serangan tertentu. Keputusan menunjukkan MFIA menyediakan peringkat keselamatan yang tinggi untuk kerangka pengurusan dalam semua piawai IEEE 802.11. Masa yang diperlukan untuk melancar serangan, menunjukkan bahawa memperuntukkan masa tertentu oleh penceroboh adalah hampir mustahil dalam model cadangan yang menyebabkan serangan tersebut tidak praktikal. Keputusan juga menunjukkan model cadangan dapat menghalang pelbagai serangan ke atas kerangka pengurusan.
ACKNOWLEDGEMENTS

Thank you God for being able to do this work, for you are all, please help me stay true to myself and my beliefs, please help me give back to all those who have given me so much. First and foremost, I would like to thank my parents, my husband, and my children for their help and support in every possible way during my life, I would be nothing without their love.

I would also like to thank my supervisor, Doctor Abdul Azim Abdul Ghani, Dean of the Faculty of Computer Science and Information Technology, for all the freedom and valuable guidance he provided me through this work. I also would like to thank Dr. Zuriati and Ms. Zaiton for serving as committee member and for providing their advices.

I wish to acknowledge Professor Vijay Garg a senior member of IEEE and an academic member of the Russian Academy of Transport in the Electrical and Computer Engineering department at the University of Illinois at Chicago who help me to answer my endless questions. I am really thankful to Dr. Nabil Afifi a lecturer in the Department of Electrical and Computer Engineering, Curtin University of Technology, Sarawak Malaysia.

Very special thanks go to Mr. Paul Andrew Johnston a master in Internet Security Specialist in England who continually helped me during this thesis. Last but not least, thanks are also due to all my classmates at University Putra Malaysia for nice academic and non-academic discussions.
I certify that an Examination Committee has met on 14th August 2007 to conduct the final examination of Mina Malekzadeh on her Master of Science thesis entitled "Security Improvement of Unicast Management Frames in IEEE 802.11 Medium Access Control Layer" in accordance with Universiti Pertanian Malaysia (Higher Degree) Act 1980 and Universiti Pertanian Malaysia (Higher Degree) Regulations 1981. The Committee recommends that the student be awarded the degree of Master of Science.

Members of the Examination Committee were as follows:

**Ali Mamat, PhD**  
Associated Professor  
Faculty of Computer Science and Information Technology  
Universiti Putra Malaysia  
(Chairman)

**Mohamed Othman, PhD**  
Associated Professor  
Faculty of Computer Science and Information Technology  
Universiti Putra Malaysia  
(Internal Examiner)

**Abdul Rahman Ramli, PhD**  
Associated Professor  
Faculty of Engineering  
Universiti Putra Malaysia  
(Internal Examiner)

**Abdul Hanan Abdullah, PhD**  
Professor  
Faculty of Computer Science and Information Systems  
Universiti Teknologi Malaysia  
(External Examiner)

---

**HASANAH MOHD. GHAZALI, PhD**  
Professor and Deputy Dean  
School of Graduate Studies  
Universiti Putra Malaysia

Date: 27 September 2007
This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Master of Science. The members of the Supervisory Committee are as follows:

**ABDUL AZIM ABDUL GHANI, PhD**  
Associate Professor  
Faculty of Computer Science and Information Technology  
Universiti Putra Malaysia  
(Chairman)

**ZURIATI AHMAD ZUKARNAIN, PhD**  
Lecturer  
Faculty of Computer Science and Information Technology  
Universiti Putra Malaysia  
(Member)

**HAJAH ZAITON MUDA, M.Sc.**  
Lecturer  
Faculty of Computer Science and Information Technology  
Universiti Putra Malaysia  
(Member)

---

**AINI IDEERIS, PhD**  
Professor and Dean  
School of Graduate Studies  
Universiti Putra Malaysia  

Date: 15 November 2007
DECLARATION

I hereby declare that the thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at UPM or other institutions.

MINA MALEKZADEH

Date: 2 September 2007
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEDICATION</td>
<td>ii</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td>iii</td>
</tr>
<tr>
<td>ABSTRAK</td>
<td>v</td>
</tr>
<tr>
<td>ACKNOWLEDGEMENTS</td>
<td>vii</td>
</tr>
<tr>
<td>APPROVAL</td>
<td>viii</td>
</tr>
<tr>
<td>DECLARATION</td>
<td>x</td>
</tr>
<tr>
<td>LIST OF TABLES</td>
<td>xiii</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td>xiv</td>
</tr>
<tr>
<td>LIST OF ABBREVIATIONS</td>
<td>xvi</td>
</tr>
</tbody>
</table>

## CHAPTER

### 1 INTRODUCTION

1.1 Background 1
1.2 Problem Statements 2
1.3 Objectives of the Research 4
1.4 Scope of the Research 4
1.5 Thesis Organization 5

### 2 IEEE 802.11 MEDIUM ACCESS CONTROL LAYER

2.1 IEEE 802.11 Topologies 8
  2.1.1 Infrastructure Network 8
  2.1.2 Ad-Hoc Network 10
2.2 IEEE 802.11 Standards and Data Rates 10
  2.2.1 IEEE 802.11b 11
  2.2.2 IEEE 802.11a 11
  2.2.3 IEEE 802.11g 12
2.3 IEEE 802.11 Layers 13
  2.3.1 Physical Layer and Modulation Methods 13
  2.3.2 Medium Access Control Layer 13
2.4 IEEE 802.11 Medium Access Control Layer Frames 14
2.5 Management Frames 15
  2.5.1 Frame Control Field 15
  2.5.2 Duration Field 17
  2.5.3 Destination, Source and BSSID Address Fields 17
  2.5.4 Sequence Control Field 18
  2.5.5 Management Frame Body 19
  2.5.6 FCS Field 24
2.6 Summary 25

### 3 SECURITY IN MEDIUM ACCESS CONTROL LAYER

3.1 WLAN State Machine 26
3.2 Data Frame Security Protocols in Medium Access Control Layer 27
  3.2.1 Wired Equivalent Privacy (WEP) 27
  3.2.2 Wifi Protected Access (WPA) 30
  3.2.3 IEEE 802.11i (WPA2) 33
## LIST OF TABLES

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Comparison of Wireless LAN Standards</td>
<td>12</td>
</tr>
<tr>
<td>2.2</td>
<td>Valid Type and Subtype combinations</td>
<td>16</td>
</tr>
<tr>
<td>2.3</td>
<td>Reason Code</td>
<td>20</td>
</tr>
<tr>
<td>2.4</td>
<td>Status Code</td>
<td>21</td>
</tr>
<tr>
<td>5.1</td>
<td>Probability of Breaking Code</td>
<td>82</td>
</tr>
<tr>
<td>5.2</td>
<td>Number of Required MFs to Forgery Attack</td>
<td>86</td>
</tr>
<tr>
<td>5.3</td>
<td>Required Time to Forgery Attack in IEEE 802.11a and g</td>
<td>90</td>
</tr>
<tr>
<td>5.4</td>
<td>Required Time to Forgery Attack in IEEE 802.11b</td>
<td>90</td>
</tr>
<tr>
<td>5.5</td>
<td>Number of Required MFs to Collision Attack</td>
<td>96</td>
</tr>
<tr>
<td>5.6</td>
<td>Required Time to Collision Attack in IEEE 802.11a and g</td>
<td>99</td>
</tr>
<tr>
<td>5.7</td>
<td>Required Time to Collision Attack in IEEE 802.11b</td>
<td>99</td>
</tr>
<tr>
<td>5.8</td>
<td>Probability of At Least One Correct RSN in Forgery and Collision Attacks</td>
<td>102</td>
</tr>
<tr>
<td>5.9</td>
<td>Security Level</td>
<td>103</td>
</tr>
</tbody>
</table>
### LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Infrastructure Network</td>
<td>8</td>
</tr>
<tr>
<td>2.2</td>
<td>Extended Service Set</td>
<td>9</td>
</tr>
<tr>
<td>2.3</td>
<td>Ad-Hoc Wireless Network</td>
<td>10</td>
</tr>
<tr>
<td>2.4</td>
<td>Wireless LAN layers</td>
<td>13</td>
</tr>
<tr>
<td>2.5</td>
<td>Management Frame Format</td>
<td>15</td>
</tr>
<tr>
<td>2.6</td>
<td>Frame Control Field</td>
<td>15</td>
</tr>
<tr>
<td>2.7</td>
<td>Sequence Control Field</td>
<td>18</td>
</tr>
<tr>
<td>2.8</td>
<td>Beacon Management Frame Format</td>
<td>19</td>
</tr>
<tr>
<td>2.9</td>
<td>Association Request Management Frame Format</td>
<td>20</td>
</tr>
<tr>
<td>2.10</td>
<td>Association Response Management Frame Format</td>
<td>21</td>
</tr>
<tr>
<td>2.11</td>
<td>Reassociation Request Management Frame Format</td>
<td>22</td>
</tr>
<tr>
<td>2.12</td>
<td>Reassociation Response Management Frame Format</td>
<td>22</td>
</tr>
<tr>
<td>2.13</td>
<td>Probe Request Management Frame Format</td>
<td>23</td>
</tr>
<tr>
<td>2.14</td>
<td>Probe Response Management Frame Format</td>
<td>23</td>
</tr>
<tr>
<td>2.15</td>
<td>Authentication Management Frame Format</td>
<td>24</td>
</tr>
<tr>
<td>3.1</td>
<td>IEEE 802.11 State Machine</td>
<td>27</td>
</tr>
<tr>
<td>3.2</td>
<td>WEP Encryption</td>
<td>28</td>
</tr>
<tr>
<td>3.3</td>
<td>TKIP Encapsulation</td>
<td>31</td>
</tr>
<tr>
<td>3.4</td>
<td>TKIP Frame Format</td>
<td>31</td>
</tr>
<tr>
<td>3.5</td>
<td>RSN Establishment Procedures</td>
<td>35</td>
</tr>
<tr>
<td>3.6</td>
<td>Cyclic Redundancy Check Process</td>
<td>38</td>
</tr>
<tr>
<td>3.7</td>
<td>Deauthentication Attack</td>
<td>43</td>
</tr>
</tbody>
</table>
4.1 The Steps Flow for the Research
4.2 The Proposed Model (MFIA)
4.3 MFIA Simulation Architecture
5.1 Output of the Proposed Model
5.2 Select the Kind of Unicast MF
5.3 Enter the MAC Addresses
5.4 Making S-code by Sender Station
5.5 Making R-code by Receiver Station
5.6 Compare the Sender and Receiver codes
5.7 Forgery Disassociation MF Attack
5.8 Making R-code in a Forged MF
5.9 Discard MF by the Proposed Model due to Forgery Insertion Attack
5.10 Breaking Code Attack
5.11 Making R-code in Breaking Code Attack
5.12 Discard MF by Proposed Model due to Breaking Code Attack
5.13 Probability of Breaking Code
5.14 Number of Required MFs to Forgery Attack
5.15 Required Time to Forgery Attack in IEEE 802.11a and g
5.16 Required Time to Forgery Attack in IEEE 802.11b
5.17 Number of Required MFs to Collision Attack
5.18 Required Time to Collision Attack in IEEE 802.11a and g
5.19 Required Time to Collision Attack in IEEE 802.11b
5.20 Probability of At Least One Correct RSN in Forgery and Collision Attacks
5.21 Security Level
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point</td>
</tr>
<tr>
<td>BSS</td>
<td>Basic Service Set</td>
</tr>
<tr>
<td>CCK</td>
<td>Complementary Code Keying</td>
</tr>
<tr>
<td>CRC</td>
<td>Cyclic Redundancy Check</td>
</tr>
<tr>
<td>DSSS</td>
<td>Direct Sequence Spread Spectrum</td>
</tr>
<tr>
<td>ESS</td>
<td>Extended Service Set</td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
</tr>
<tr>
<td>FHSS</td>
<td>Frequency Hopping Spreading Spectrum</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>ISM</td>
<td>Industrial Science Medicine, refers to 2.4 GHz unlicensed Frequency band</td>
</tr>
<tr>
<td>MAC</td>
<td>Message Authentication Code</td>
</tr>
<tr>
<td>MFIA</td>
<td>Management frame with Integrity and Authenticity</td>
</tr>
<tr>
<td>OFDM</td>
<td>Orthogonal Frequency Division Multiplexing</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hash Algorithm</td>
</tr>
<tr>
<td>TKIP</td>
<td>Temporal Key Integrity Protocol</td>
</tr>
<tr>
<td>UNII</td>
<td>Unlicensed National Information Infrastructure, refers to 5 GHz Unlicensed Frequency Band</td>
</tr>
<tr>
<td>WEP</td>
<td>Wired Equivalent Privacy</td>
</tr>
<tr>
<td>WPA</td>
<td>Wireless Protected Access</td>
</tr>
</tbody>
</table>
CHAPTER 1
INTRODUCTION

1.1 Background

Over the past several years, wireless technology has changed the way people communicate. In particular, the wireless network technology has become so popular that it has already been accepted as an easy alternative to wired networks. Some of the advantages of the wireless network technology are: available network access without wires everywhere, high data rates, and less price in contrast to wired networks.

Among the wireless network technologies, Wireless Local Area Network (WLAN) or IEEE 802.11 is more popular. The IEEE 802.11 working group was formed in 1990 and its goal was to create a WLAN that operates in one of the Industrial, Scientific, and Medical (ISM) frequency ranges.

The first IEEE 802.11 standard was released in 1997 (Henley, 2000) and after that three other standards IEEE 802.11a,b, and g were released. IEEE 802.11 uses radio frequency to transmit and receive data over the air by exchanging three kinds of frame: control, data and management frame.

With rapidly growing of the WLANs, security is very important for a safe communication between wireless stations. Therefore different protocols have been
designed to provide security for all IEEE 802.11 standards.

Unfortunately these protocols only put much attention on securing data frames, and less on securing management frames and control frames. Currently, management frames use Cyclic Redundancy Check (CRC-32 bit) algorithm for security but CRC is useful only for unintentional error detection of the management frames and cannot provide any security in form of authentication or privacy.

Hence an unprotected management frame can be used by intruder to start different attacks like injecting new forgery management frames, modify existing management frames, denial of service attack and other kinds of attack on management frames to break into the whole WLAN.

Thereby, this thesis presents a new model to provide a strong security mechanism to avoid possible common attacks on management frames, which is called Management Frame with Integrity and Authentication (MFIA).

1.2 Problem Statements

IEEE 802.11 provides strong security for data frames but control and management frames are transmitted without any protection. Management frames are transmitted in form of request and response. This means, a sender transmits management frame request and then receives related management frame response. Whereas control frames are transmitted as exchanging for data frames. Control frames do not carry
important information and generally they are used to acknowledge data frames. Since management frames do not apply any control frame in their transmission (ANSI IEEE 802.11, 1999) therefore this research attempts to propose a new model to provide sufficient security for management frames.

The current security for management frames is CRC algorithm which can not protect management frames against malicious attacks (Sood and Eszenyi, 2006; Bellardo and Savage, 2003). Hence, the following problems on management frames have been identified:

- Management frames will be accepted easily by the receiver who carries out the specified function of the management frame without checking whether the sender is a legitimate user or if the management frame has not been modified during transmission. In this situation an intruder can easily spoof these frames and send forgery management frames as an authorized user to launch different kinds of attack.

- There is a sequence number field in the header of management frames. This field is a sequential number and it ranges from 0 to 4095 and gets reset every time the station restarts. The sequence numbers are predictable and are not encrypted. Therefore with knowledge of the current sequence number, the adversary can easily set a proper sequence number for his forgery management frames (Wright, 2003).
1.3 Objectives of the Research

This research has two objectives:

- To design and implement a new model to provide a strong security for management frames in WLAN. This proposed model has two main functions: authentication of the sender and integrity of the management frame. In case of a successful authentication and integrity, the receiver will accept the original management frame. Any problem during authentication and integrity process causes the receiver to assume there is an attack on the management frame and discards it.

- To add a new Random Sequence Number (RSN) to avoid an intruder easily set a proper sequence number for his forgery management frame. The proposed model produces a random sequence number to make the MFIA more difficult to figure out by an intruder. This means an intruder will need more attempt in guessing the correct value of the random sequence number therefore makes the proposed model stronger.

1.4 Scope of the Research

This research considers unicast management frames to protect. They are chosen because currently the most important problems of the management frames are forgery and collision attacks which are basis of other types of attack. On the other hands these two important attacks can be started just by using unicast management
frames because of their specified functions. Unicast management frames can be used by intruder to change one of the addresses in their header to use the functions. For example by changing the destination address in the header of a disassociation management frame to a broadcast address intruder can force all the stations in the WLAN to be disconnected from the network.

Hence an unprotected unicast management frames provide a powerful arsenal to an attacker, who can discover the layout of the network, find the location of devices and start more successful denial-of-service attacks against a network (Epstein, 2006; Wright, 2007).

But role of the broadcast management frames is different and they are rarely used. These frames typically are used to adjust radio frequency properties or find a proper access point for stations, rather than report sensitive information (Epstein, 2006; Wright, 2007).

1.5 Thesis Organization

This thesis is divided into 6 chapters. The first chapter shows a background of the problem that this research tries to solve. The objectives of this research are also stated in this chapter.

Chapter 2 provides an introduction to IEEE 802.11 topologies and standards. It explains the two basic wireless network layers, physical and medium access control
layer, and different techniques for transmission data over these two layers. It also discusses all kinds of wireless network frame and their functions.

Chapter 3 explains existing security protocols in IEEE 802.11 medium access control layer. It presents security process; authentication, confidentiality and integrity, in the mentioned protocols. It shows the current algorithm to protect management frame and also describes common current security threats and vulnerabilities on management frames. This chapter shows related works that have been done before in relation to the problem of management frames.

In chapter 4 the proposed model is introduced to improve and enhance security of the management frames and then the proposed model will be simulated by a program in JavaScript and HTML. Step taken in the source code of the program also is shown in this chapter.

In chapter 5, first the proposed model will be implemented to show its correctness and after that it will be evaluated to show its effectiveness to enhance the security of the wireless networks, and then a comparison between the proposed model and current algorithm (CRC) will be discussed. It also will show the result of the comparison of the proposed model against the current algorithm and will discuss the probability of different kinds of common attack on them.

Conclusion will be discussed in chapter 6 and it explains the strength of the
proposed model to prevent a variety of common attacks related to management frames and then it proves the proposed model can enhance the security of the entire WLAN. Finally it states the contributions of this research and suggests future works to improve security of WLANs.
CHAPTER 2
IEEE 802.11 MEDIUM ACCESS CONTROL LAYER

This chapter provides descriptions of WLAN topologies and its standards and also describes IEEE 802.11 layers with their related frames.

2.1 IEEE 802.11 Topologies

Two network topologies are defined in the IEEE 802.11: infrastructure network and Ad-Hoc network (Arbaugh et al., 2001). In fact, the difference between them is only in how the devices communicate to each other.

2.1.1 Infrastructure Network

An infrastructure WLAN (which is the focus of this thesis) consists of several clients talking to an Access Point (AP) which is usually connected to a wired network like home LAN. IEEE 802.11 is based on a cellular architecture where the system is subdivided into cells. Each cell called Basic Service Set (BSS) which is controlled by an AP. So infrastructure mode of operation also is called a BSS (Xiao et al., 2004). This is shown in Figure 2.1.

Figure 2.1: Infrastructure Network