Bachelor's Thesis (TUAS)

Degree programme in Information Technology

Specialisation: Internet Technology

2015

Waheed Gandonu

IMPROVING WIRELESS NETWORK DEPENDABILITY FOR END-USERS

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR'S THESIS (UAS) │ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information Technology | Internet Technology

Spring 2015 | 34

Instructor: Patric Granholm

Waheed Gandonu

IMPROVING WIRELESS NETWORK DEPENDABILITY FOR END-USERS

Wireless network dependability has become an important issue for service providers, vendors, and users since everyone from all walks of life depends on wireless network and mobile services. To improve a wireless network, reliability, availability, and security are the main aspects of network dependability to be considered because wireless networks are more likely to have dependability problems in the future.

This thesis focuses on the main aspects to wireless network dependability and also proposes an integrated approach using design changes and fault-tolerance to improve the dependability of wireless network.

KEYWORDS:

Dependability, Reliability, Availability, Security, Wireless.

TABLE OF CONTENTS

FIGURES

LIST OF ABBREVIATIONS

BS	Base Station
BSC	Base Station Controller
BTS	Base Transceiver Station
DNS	Domain Name System
E.I.R.P	Equivalent Isotropically Radiated Power
HLR	Home Location Registers
IEEE	Institute of Electrical and Electronic Engineers
IPS	Intelligent Protection Switching
LTE	Long Term Evolution
MAC	Media Access Control
MSC	Mobile Switching Center
MTBF	Mean Time Between Failure
MTTR/MTR	Mean Time To Restore/Recovery
MTTF	Mean Time To Failure
GSM	Global System for Mobile
NAC	Network Admission Control
PSTN	Public Switched Telephone Network
QoS	Quality of Service
VLR	Visitor Location Register

VPN	Virtual Private Network
WAP	Wireless Application Protocol
WEP	Wired Equivalent privacy
WPA	WI-FI Protected Access
WIMAX	Worldwide interoperability for Microwave Access
WLAN	Wireless Local Area network
WIB	Wireless Infrastructure building-Block

1 INTRODUCTION

Network dependability needs a different field of requirements each of must be realized by combining efficient and qualified technologies. High dependability systems are based on these categories: Reliability, Availability, Integrity and Security. The dependability of a wireless network relies on the ability to diagnose and recover faults which result from the following: network misconfiguration (e.g., VLAN, BGP, NAT, or DHCP misconfiguration), hardware problems (e.g., malfunctioned router interface, physical link disconnection), and software errors.

Tools such as Trace Route can be used to diagnose network problems, and the results of these tools can be used to decide what can be done to solve the problem. Network administrators/engineers have diverse tools and techniques in solving wireless network issues related to wireless security, accessibility, reliability, and efficiency. The goal of this thesis is to examine methods to diagnose as many wireless network faults as possible, and to make wireless networks more dependable and reliable for its users.

2 OVERVIEW OF NETWORK DEPENDABILITY ANALYSIS

2.1 Dependability

Network dependability is the ability of a system to deliver its required level of service to its users, especially in the light of failures or other incidents that impose on its level of service. It can be viewed as the system reliability, availability, safety and maintainability. Depending on the application environment, one or more of these characteristics is an appropriate reflection of the system behavior. The details of the analysis can be found in Figure 1 below.

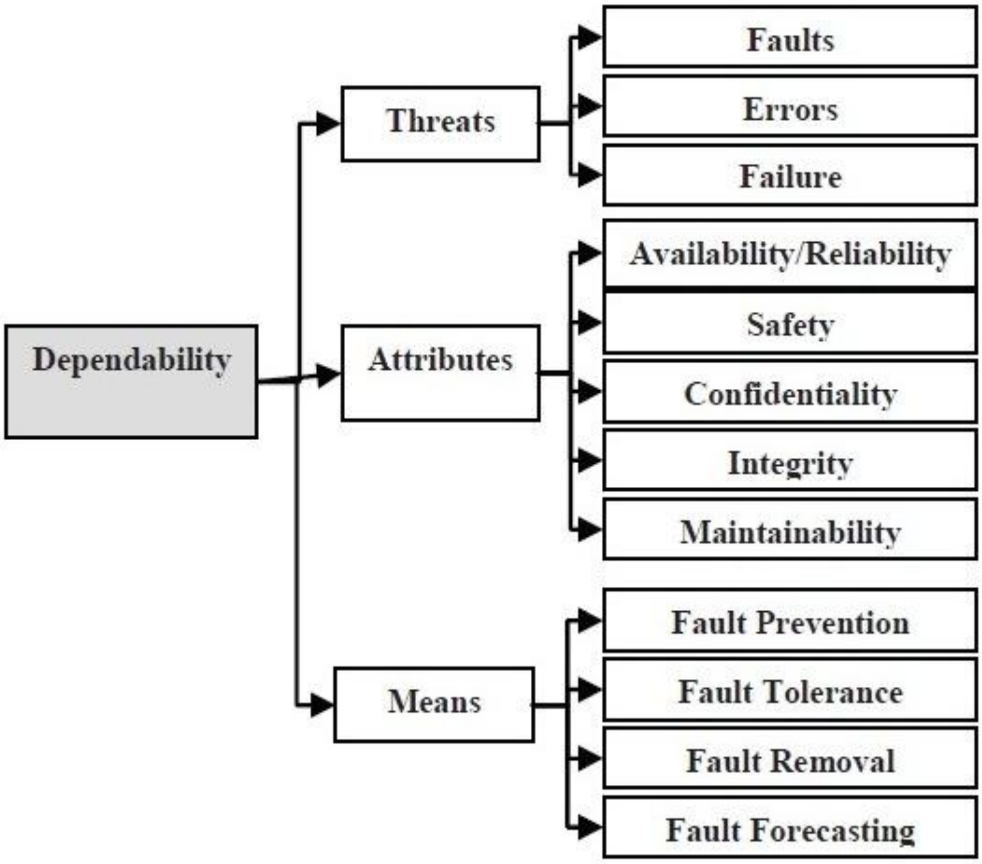


Figure 1. Network Dependability Concept (Al-kuwaiti et al., 2009).

2.2 Reliability

Reliability is the ability of a network to give its required functions to the users under stated conditions at the accessing time. It can also be defined under a conditional probability that the network will perform its required functions without failure at anytime provided it is fully operational at that time (Al-kuwaiti et al., 2009).

To obtain a reliable network, network engineers implement reliability into every component from the start of the network design. Four important features must be introduced and implemented at the starting phase of the design to achieve reliable and available systems; fault-avoidance, fault-tolerant, fault-detection, and fault-restoration (Al-kuwaiti et al., 2009). Figure 2 below shows the reliability concept in a network.

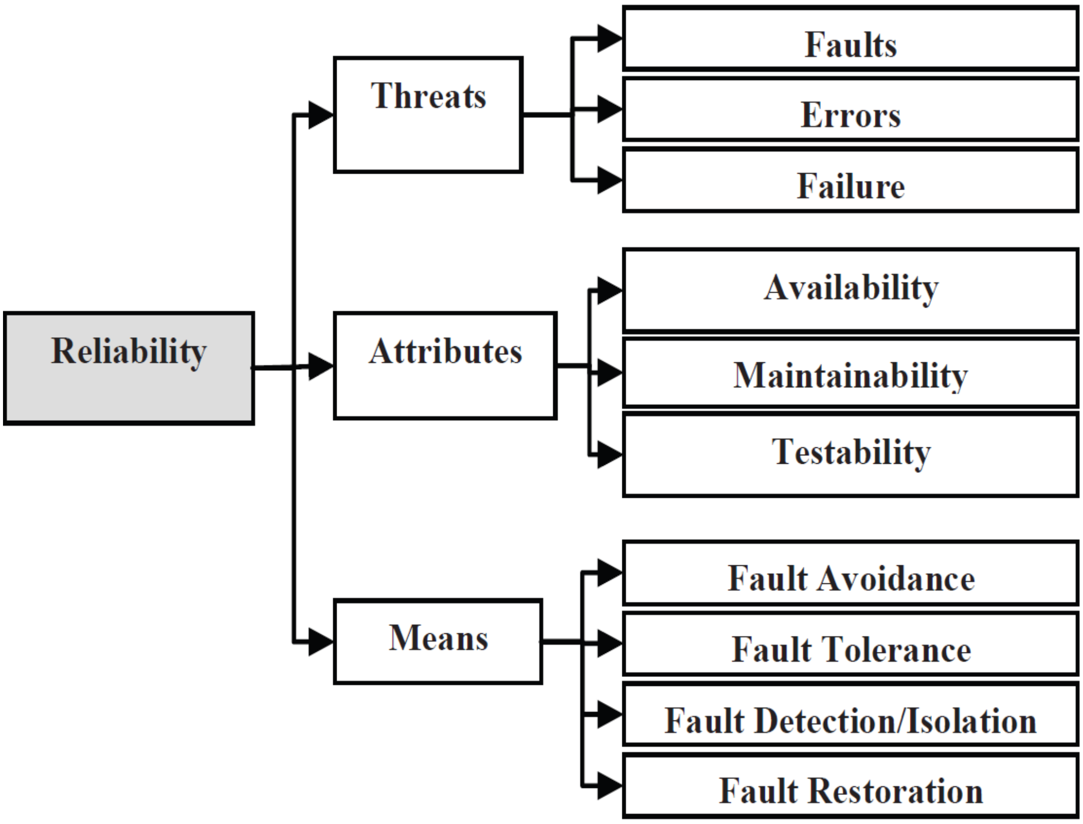


Figure 2. Network Reliability Concept (Al-kuwaiti et al., 2009).

2.3 Fault Tolerance

Fault-tolerance is the ability of a network to continue its required operation, despite the faults of hardware or software at specific period of time. Fault-tolerance is for a network to have the capability to continue the correct execution of its output functions in the presence of faults. Fault tolerance is a means to achieve dependability and reliability in a network (Al-kuwaiti et al., 2009).

The process of restoring the network to its fully operational condition is called reconfiguration. Network engineers use the reconfiguration process, when there are VLAN mismatches, security issues, cable interchanges, but must be aware of the fault detection, fault location, fault containment, and fault recovery. (Al-kuwaiti et al., 2009). Figure 3 below shows the fault-tolerance concept in a network.

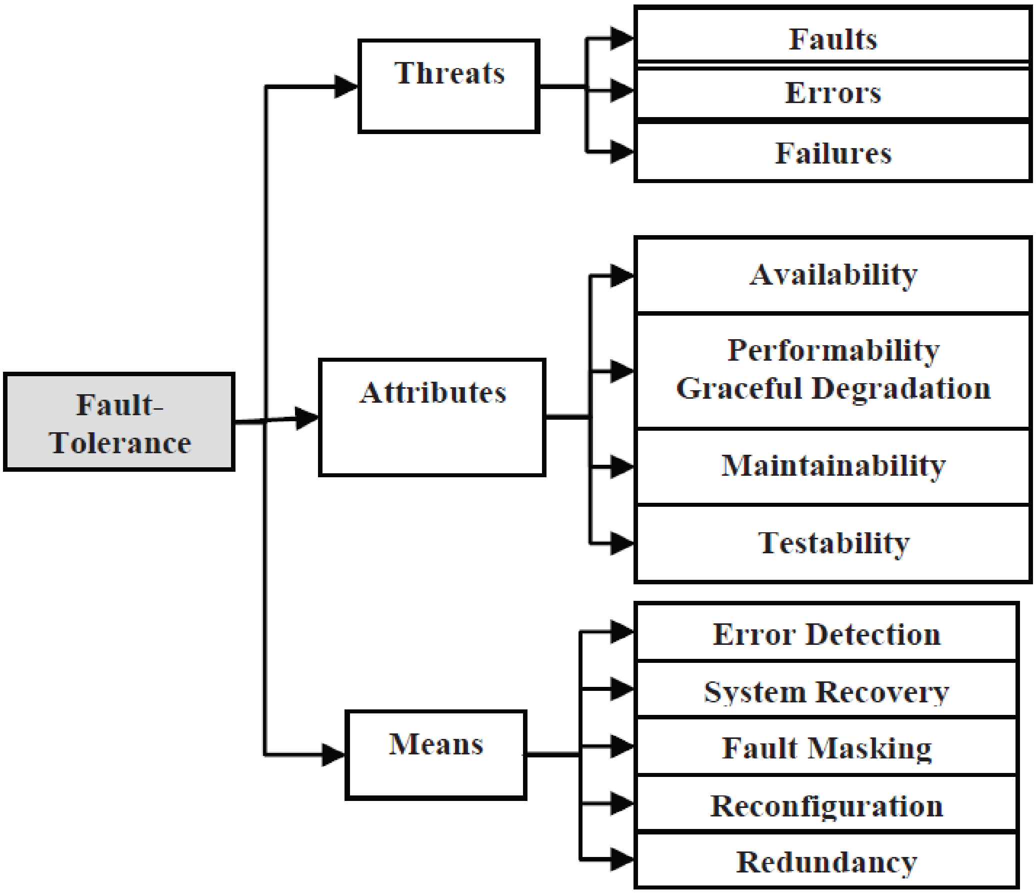


Figure 3. Network Fault-Tolerance Concept (Al-kuwaiti et al., 2009).

2.4 Security

Security refers to any implemented policy, activities designed, or information given to secure or to protect the network. All these ensure that the usability, reliability, integrity, and safety of the network are been protected. Network security stops all kinds of attacks from entering or spreading on the network.

- The common network security threats are:
- Viruses and Spyware
- Hacker attacks
- Denial of service attacks (DOS)
- Data interception
- Identity theft.

The following network security components are used to prevent and secure the network from an unauthorized access or attacks:

- Anti-virus and anti-spyware
- Firewall
- Intrusion protection systems (IPS) and Intrusion detection system (IDS)
- Virtual Private Networks (VPNs)

Figure 4 below shows the security concept in a network.

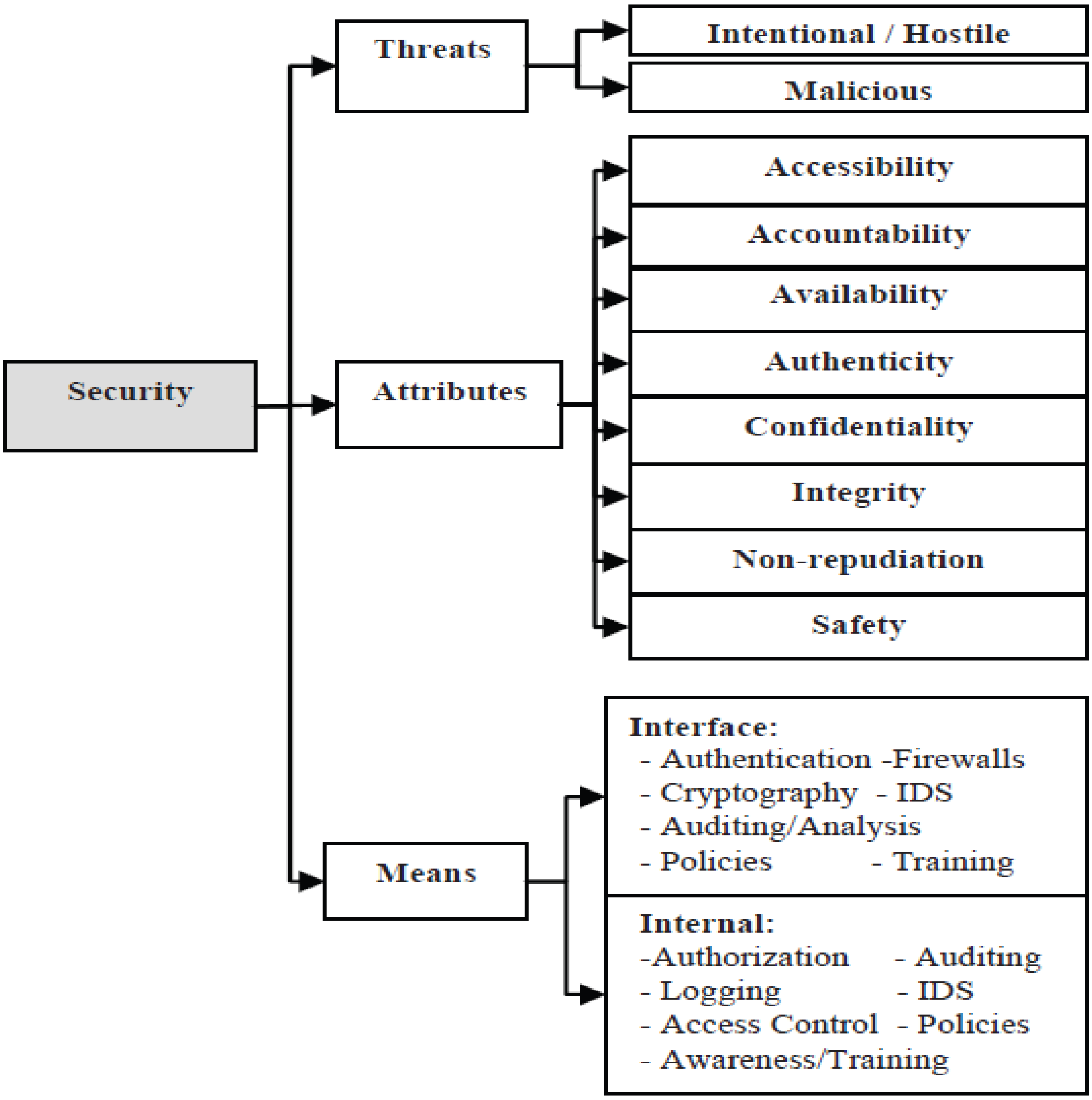


Figure 4. Network Security Concept (Al-kuwaiti et al., 2009).

3 MODELING AND PERFORMANCE EVALUATION

3.1 Reliability Modeling and Analysis Methods

A reliability analysis analyses the functionality performance of a wireless network. It performs an important measure and high level of reliability requirement for wireless networks. The reliability level of a wireless network can be evaluated using a tool called reliability modeling. Reliability modeling and analysis are steps in designing and optimization of wireless network systems. This approach for establishing the reliability of a highly reliable Wireless Network, is

- To develop an arithmetical model of the reliability measure of the network
- To determine the specifications of the model, and
- To assess the network reliability based on the model and the specified frameworks.

Reliability modeling is used to predict the performance of the network tools and to provide the information for the design of wireless network suitable for connection. For a network already deployed in the field, reliability modeling combined with failure data analysis, can be used to identify the critical components, apply fault tolerance and enhance reliability (Venkatesan et al., 2013).

3.1.1 Reliability Measure

Reliability measure is the degree to which a network can be depended on to secure and consistent results upon repeated application. This measure also depends on the network and its applications (Venkatesan et al., 2013). There are situations to be considered when measuring the reliability of a wireless network. They are as follows:

- Connectivity Reliability Measure: There are three main network connectivity reliability problems: two-terminal, K-terminal and all-terminal reliabilities (Kharbash and Wang, 2007; Venkatesan et al., 2013).

- Hardware Reliability Measures: These are MTTR, MTTF, and MTBF.

  MTBF (Mean Time Between Failures) refers to the amount of time that elapses between one failure and the next. That is, the sum of MTTF and MTTR, the total time required for a device to fail and that failure to be repaired.

  The mean time to failure (MTTF) of a system is the expected time until the existence of the system fails. If X is a random variable that represents the time to existence of system failure, then MTTF = e[x] (Hneiti and Ajlouni, 2006).
- QoS Reliability Measure:- the measure of a service quality that the network offers to the users (Venkatesan et al., 2013; Dazhi and Pramad, 2004).
- Information Reliability Measure:- This ensures that the nodes transmit the require data and information for the user (Venkatesan et al., 2013).
- Capacity Measure:- Is understood to be the probability that the strength of the network is greater than the demand (Venkatesan et al., 2013).

Reliability measures ensure that wireless network provide the desired services to the end user without forgetting the quality of service (QoS).

3.1.2 Availability Measures

Availability of a wireless is to access it at a given time or at any instant of time without any delay, knowing that the external resources, if required, are provided. System availability measures are especially relevant in repairable systems, sometimes interruptions in service are tolerated (Hneiti and Ajlouni, 2006).

- The availability A(t) of a system at time t is the probability that the system is functioning correctly at time t. Availability A(t) functions with normal time t and probability R(t) or with the last repair time x, i.e. $0 < x < t$ and R(t).

  Availability and Reliability are related but different. i.e; $A(t) \geq R(t)$

- The steady-state availability A_{ss} represents the long-term probability that the system is available:

  i.e $A_{ss} = \frac{MTTF}{MTTF+MTTR}$ (1)

4 FACTORS INFLUENCING THE DEPENDABILITY OF A WIRELESS NETWORK

There are factors that can affect Wireless Network performance which depend mainly on the technology of the devices used, the local and geographical environment, the signals which they travel through and the fundamental physics behind wireless transmission. These factors could cause some negative effect on the network performance and the users if not stopped or avoided. Others factors can be minimised by upgrading wireless equipments with the latest technology or good network planning.

Factors that can affect Wireless Network performance are listed below but few are to be discuss (4gon, 2014):

1. Physical Obstacles
2. Wireless Range and Distance Covered
3. Wireless Network Interference
4. Signal Sharing
5. Wireless Speed and Usage
6. Antennas and Signal Polarization
7. Environmental Factors
8. Spectrum Channel Limitations
9. Signal Reflection
10. Wireless Signal Restriction
11. Backwards & Forwards Compatibility and Standards

4.1 Physical Obstacles

Trees, buildings, hills, concrete and steel walls are example of physical obstacles. These obstacles weaken or prevent wireless signals. It is very hard sometimes for wireless signals to pass through these obstacles and maintain the exact coverage. Physical obstructions reduce the range of a wireless network by 15% or more.

4.2 Wireless Range and Distance Covered

The more distance between the two devices that are trying to communicate with each other, the more the signal strength drops and vice versa. Wireless range extenders help to keep connecting devices connected to the network with a reliable connection, strong signals and expanded coverage.

The signal strength decreases base on the efficient of the two devices but mainly in an inverse cubic relation with respect to the distance between the two devices (4gon, 2014).

That is:

$$\text{Signal Strength} = \frac{1}{Distance^3} \qquad (2)$$

4.3 Wireless Network Interference

Wireless network interference can be radio frequency or electrical interference. Since a wireless network operates over radio frequencies which are 2.4 GHz and 5 GHz, devices such as microwave ovens and other wireless equipments that operate on the same frequency can cause interference with each other (Clublinks, 2015). This might have some negative impact on the performance of the network. Refrigerators, computers, fans, are devices that can cause electrical interference. The impact they have on the signal depends on the proximity of the electrical device to the wireless access point.

4.4 Signal Sharing

The sharing of signal or connection occurs when many subscribers uses the network at the same time. This means that the access point has more devices to communicate with at the same time.

4.5 Wireless Speed and Usage

The more users are accessing the network bandwidth, the less network bandwidth there is share among them. Bandwidth traffic monitoring can be used to analyse and monitor network performance and traffic. This controls the percentage of network bandwidth used on each website or application. Video streaming applications or websites utilise more bandwidth. To keep the speed and performance of a reliability network at a very high level, investing in an efficient equipments is the only solution.

4.6 Antennas and Signal Polarization

The function of antennas is to control the direction of how transmitted signals are spread or broadcast. The installation or mounting of antennas is to enhance network performance for easy accessibility. There are three common antenna types: omni-directional, directional, and semi or highly directional antennas. Omni-directional antennas are easy to install and transmit signal on one plane but propagate in all directions (4gon, 2014). Directional antennas are mostly placed in the corner of a room which propagate all the room. Semi-directional antennas are used in for cellular communication because they can propagate in a very narrow way.

4.7 Environmental Factors

Weather conditions, fog, floods, and rainstorms can cause one of the biggest effect on wireless signals. These can have negative impact on the reliability of the signal and may cause greater subsidence, damaging masts and underground cables. These factors may also cause a wireless network infrastructure to be flooded, or damaged by an increase in trees falling onto overhead lines.

4.8 Spectrum Channel Limitations

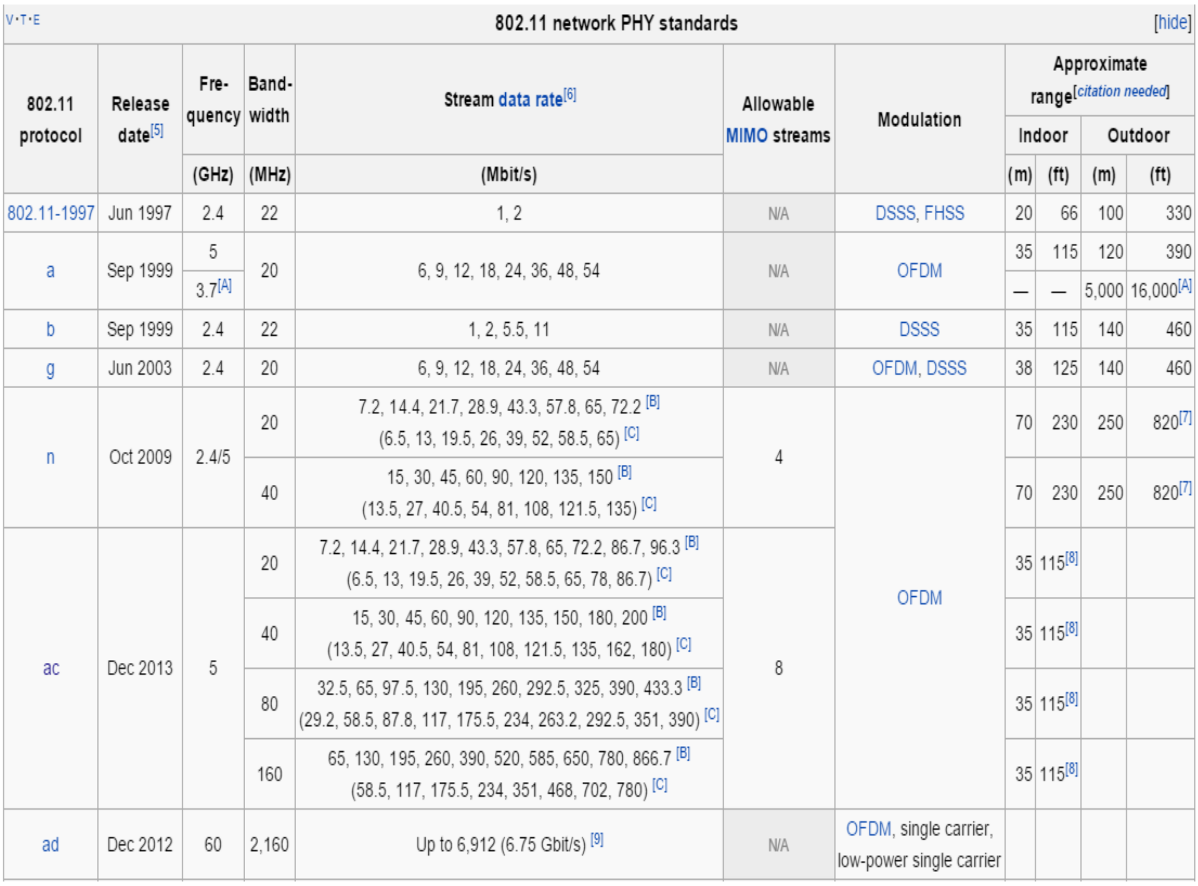
Spectrum channel limitations affects on wireless networks that operate on frequency bands of 2.4GHz and will start to have effect on the 5GHz bands in the future if people migrate in mass (4gon, 2014). Channels are the sub-bands frequency which wireless networks operate on, they are of smaller bandwidths within their operating frequencies.

4.9 Wireless Signal Restriction

Due to security reasons, or network usage, restricting wireless signal transmission might have a negative effect on the signal strenght of the network (Clublinks, 2015).

4.10 Backwards & Forwards Compatibility and Standards

Wireless network devices needs to be upgraded, when old devices are not compatible with the latest ones. Replacing old devices will enhance the full potential of new standards of technology. The wireless network operate on 802.11 standards. The 802.11ac is the latest.



V·T·E 802.11 network PHY standards [hide]

802.11 protocol	Release date[5]	Fre-quency	Band-width	Stream data rate[6]	Allowable MIMO streams	Modulation	Approximate range[citation needed]			
							Indoor		Outdoor	
		(GHz)	(MHz)	(Mbit/s)			(m)	(ft)	(m)	(ft)
802.11-1997	Jun 1997	2.4	22	1, 2	N/A	DSSS, FHSS	20	66	100	330
a	Sep 1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	N/A	OFDM	35	115	120	390
		3.7[A]					—	—	5,000	16,000[A]
b	Sep 1999	2.4	22	1, 2, 5.5, 11	N/A	DSSS	35	115	140	460
g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	N/A	OFDM, DSSS	38	125	140	460
n	Oct 2009	2.4/5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2 [B] (6.5, 13, 19.5, 26, 39, 52, 58.5, 65) [C]	4	OFDM	70	230	250	820[7]
			40	15, 30, 45, 60, 90, 120, 135, 150 [B] (13.5, 27, 40.5, 54, 81, 108, 121.5, 135) [C]			70	230	250	820[7]
ac	Dec 2013	5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7, 96.3 [B] (6.5, 13, 19.5, 26, 39, 52, 58.5, 65, 78, 86.7) [C]	8		35	115[8]		
			40	15, 30, 45, 60, 90, 120, 135, 150, 180, 200 [B] (13.5, 27, 40.5, 54, 81, 108, 121.5, 135, 162, 180) [C]			35	115[8]		
			80	32.5, 65, 97.5, 130, 195, 260, 292.5, 325, 390, 433.3 [B] (29.2, 58.5, 87.8, 117, 175.5, 234, 263.2, 292.5, 351, 390) [C]			35	115[8]		
			160	65, 130, 195, 260, 390, 520, 585, 650, 780, 866.7 [B] (58.5, 117, 175.5, 234, 351, 468, 702, 780) [C]			35	115[8]		
ad	Dec 2012	60	2,160	Up to 6,912 (6.75 Gbit/s) [9]	N/A	OFDM, single carrier, low-power single carrier				

Figure 5. IEEE 802.11 network standard (Wikipedia, 2015a).

5 IMPROVING THE DEPENDABILITY OF A WIRELESS NETWORK

Two approaches will be discussed here on how to improve the dependability of wireless networks. The first one is based on design changes, while the second one uses fault-tolerance to enhance the wireless dependability attributes.

5.1 Design and components

Wireless networks can be improved with the helps of design change or establishing a faster recovery time which could enhance wireless network dependability for the users. This can be achieved by deploying more reliable and efficient components and changing how they are connected to each other.

Improving dependability is performed by avoiding failures as much as possible for efficient performance. To know how design changes can improve wireless network dependability, a Building Block approach is used (Varshney and Malloy, 2001). This approach uses a Wireless Infrastructure Building Block which contains a Home Location Register, Visitor Location Register, Base Station Controllers, Mobile Switching Center and Base Stations (Varshney and Malloy, 2001).

The components of Mean-Time-To-Restore will be reduced and that of Mean-Time-Between-Failure will be increased in order to enhanced or improved the wireless dependability. In addition, changing the number of levels in blocks, number of components or size of infrastructure blocks will have a positive impact on one or more of the dependability attributes. This approach uses a multiple building blocks of different components, sizes, and levels. Any of these can optimize any of the dependability attributes.

5.2 Fault- Tolerance

Fault-tolerance is the ability of a system to continue its operation even in the presence of component or system failures. To improve wireless network dependability, fault-tolerance can be used in one or several phases of the network such as switch, block, device, cell, and inter-network (Varshney and Malloy, 2001). This can be achieved or introduced with a different approach.

- The use of multiple interfaces can be achieved at device level. This will merge interfaces to different or same networks.
- The use of multiple base stations can be introduced at cell level.
- The use of fault tolerant architecture like SONET ring (Varshney and Malloy, 2001) can be introduced at switch level. This will result in the switches having internal redundancy of one or more components. A base station can also be connected to more than one switch to overcome failure of the switches.
- Fault tolerance at the block level is needed due to failure of one or more links connecting several blocks together.

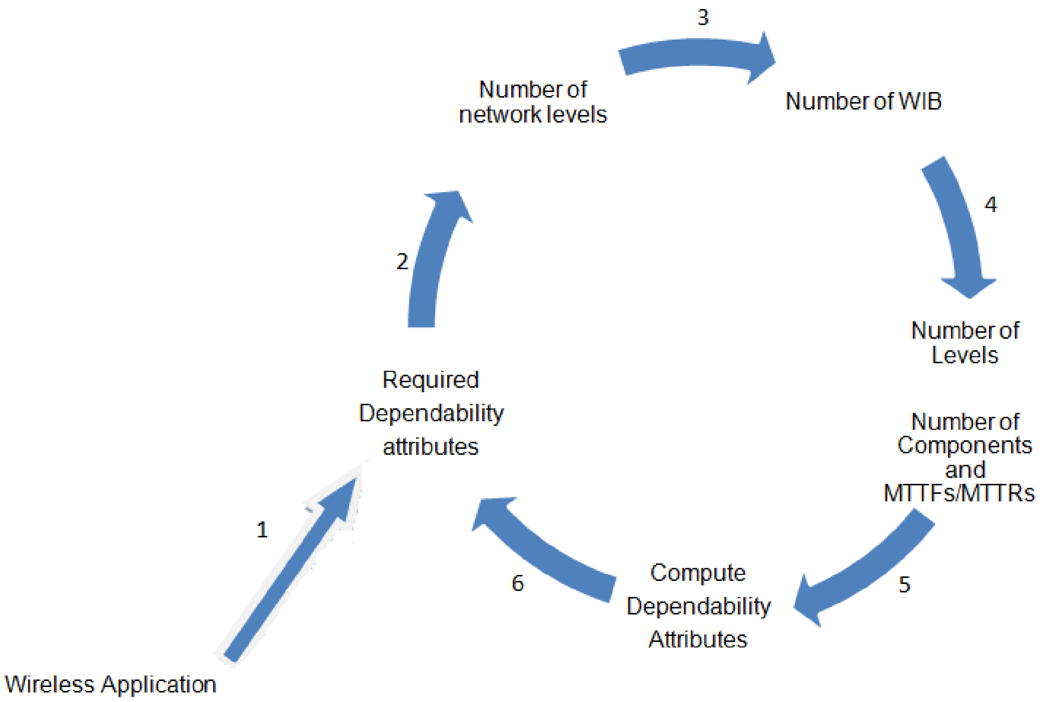

3
Number of network levels
Number of WIB
4
2
Number of Levels
Required Dependability attributes
Number of Components and MTTFs/MTTRs
1
6
5
Compute Dependability Attributes
Wireless Application

Figure 6. An approach to improving wireless dependability.

6 TYPES AND PERFORMANCE OF WIRELESS NETWORK

There are several wireless technologies in use: Wi-Fi, Bluetooth, Zig Bee, HSPA, LTE, G standards, WiMAX, satellite services, and more.

6.1 WLANs (Wireless Local Area Networks)

WLANs use radio waves to connect wireless devices to the internet without the use of cables. e.g., WiFi.

Wi-Fi can be connected over the air, using radio waves. It includes radio frequency spectrum, end user devices (e.g laptops), and network infrastructure to connect to the internet.

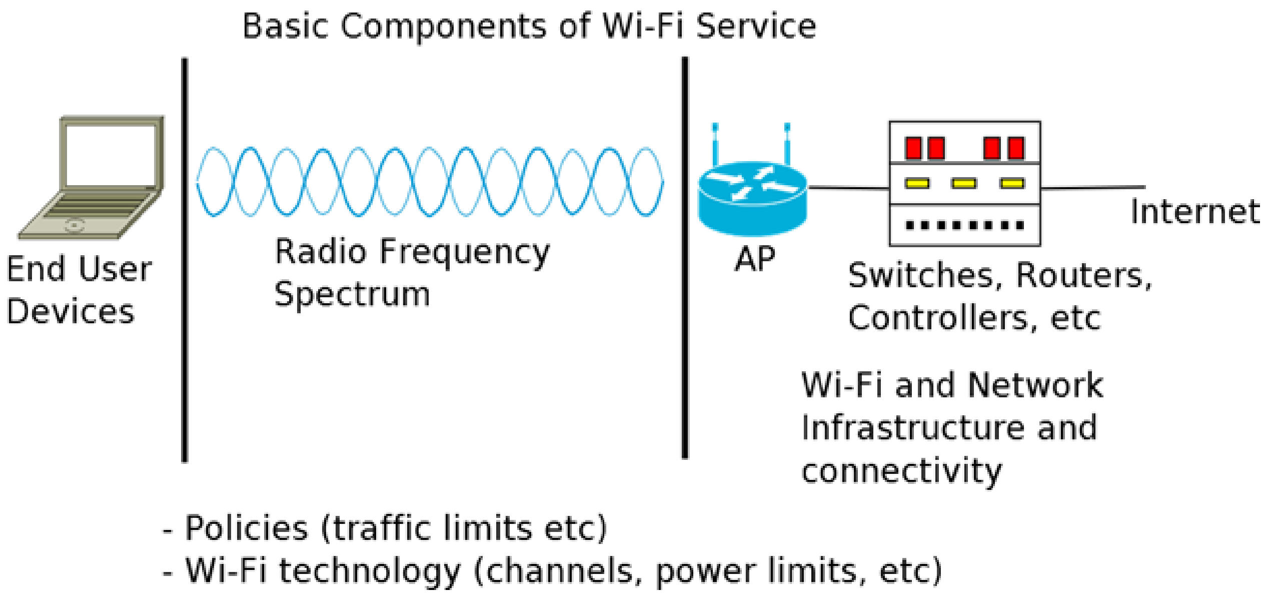

Basic Components of Wi-Fi Service
End User Devices
Radio Frequency Spectrum
AP
Switches, Routers, Controllers, etc
Internet
Wi-Fi and Network Infrastructure and connectivity
- Policies (traffic limits etc)
- Wi-Fi technology (channels, power limits, etc)

Figure 7. Basic components of Wi-Fi service

This type of network has a specification and standards assigned by IEEE which are: 802.11a, 802.11b, 802.11n 802.11g, and 802.11ac. These standards operate by transmission of voice, data and video using radio frequency.

Wi-Fi uses 802.11 standards to create a wireless local-area network that is secure, affordable for homes, company or an organization network use. Wi-Fi network is the connection of wireless router to the Internet through a wired network connection, the wireless router transmits and receives data from each device, and connects them together and to the outside world.

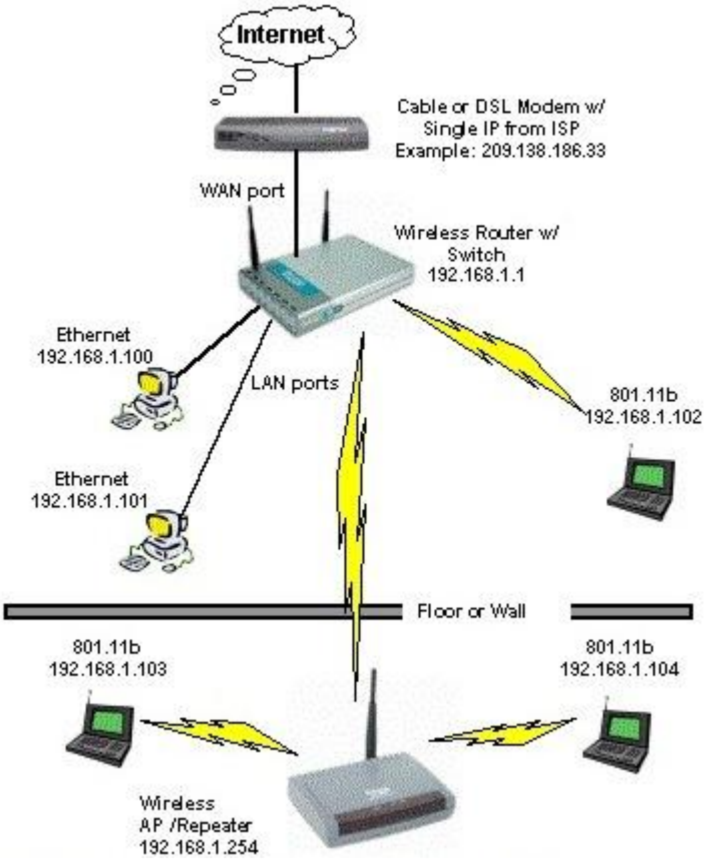


Figure 8. Network diagram with Wireless and Wired components

6.2 PANs (Personal Area Networks)

There are two types of this kind of network: Infra-Red (IR) and Bluetooth (IEEE 802.15). The connection of wireless devices for this network is within the area of about 10 meters for Bluetooth and IR connecting range is less because it requires direct line of site

Bluetooth is the wireless technology that can be used to establish an ad-hoc connection between wireless or mobile devices to transfer data or voice within a short distance in low bandwidth without the use of cables (technopedia, 2014b). This technology operates between 2.402 and 2.485 GHz on a microwave radio frequency spectrum with a speed up to 3 Mbps which can connect atleast 5 devices simultaneously.

Bluetooth works at different levels: It establishes connection at the physical level. It also establishes an agreement at the protocol level, where devices agree on when and how many bits are sent at a time. It also ensures that the message received is the same as the message sent.

To secure Bluetooth devices, the user must connect to a trusted device before exchanging data. This is where the device-level and the service-level security work together to secure Bluetooth devices from unauthorized data transmission.

.

Figure 9. Bluetooth connections.

Infrared is a wireless technology used to connect mobile devices over very short distances. An IR connection has a restriction because it requires line-of-sight, i.e., a short transmission range and is unable to penetrate walls (Technopedia, 2014).

Infrared Data Association (IrDA) devices can only exchanged connection on a one-to-one basis. Data or voice messages transmitted between IrDA devices are always unencrypted.

Light-emitting diodes (LED) are used to transmit IR signals, which pass through a lens and focus into a beam of IR data. e.g., used in television remote control.

6.3 MANs (Metropolitan Area Networks)

Metropolitan area network is a connection of several networks where copper laying or fiber cablings are used. It is a connection between different buildings in a city, e.g., WiMAX.

WiMAX (Worldwide Interoperability for Microwave Access) is a telecommunications protocol describing fixed and fully mobile Internet access services. This technology allows ISPs and carriers to provide Internet connectivity to homes or offices without cabling or wiring to the user's premises (technopedia, 2014a). It is the IEEE specification of 802.16 Standard.

WiMAX has two parts: WiMAX tower and WiMAX receiver.

The WiMAX tower provides coverage to a very large area. It connects to the Internet using a high bandwidth and wired connection (a T3 line connection). It can also connect to another WiMAX tower using a "line of sight" or microwave link. The WiMAX receiver and antenna can be built into a laptop or in form of a PC card.

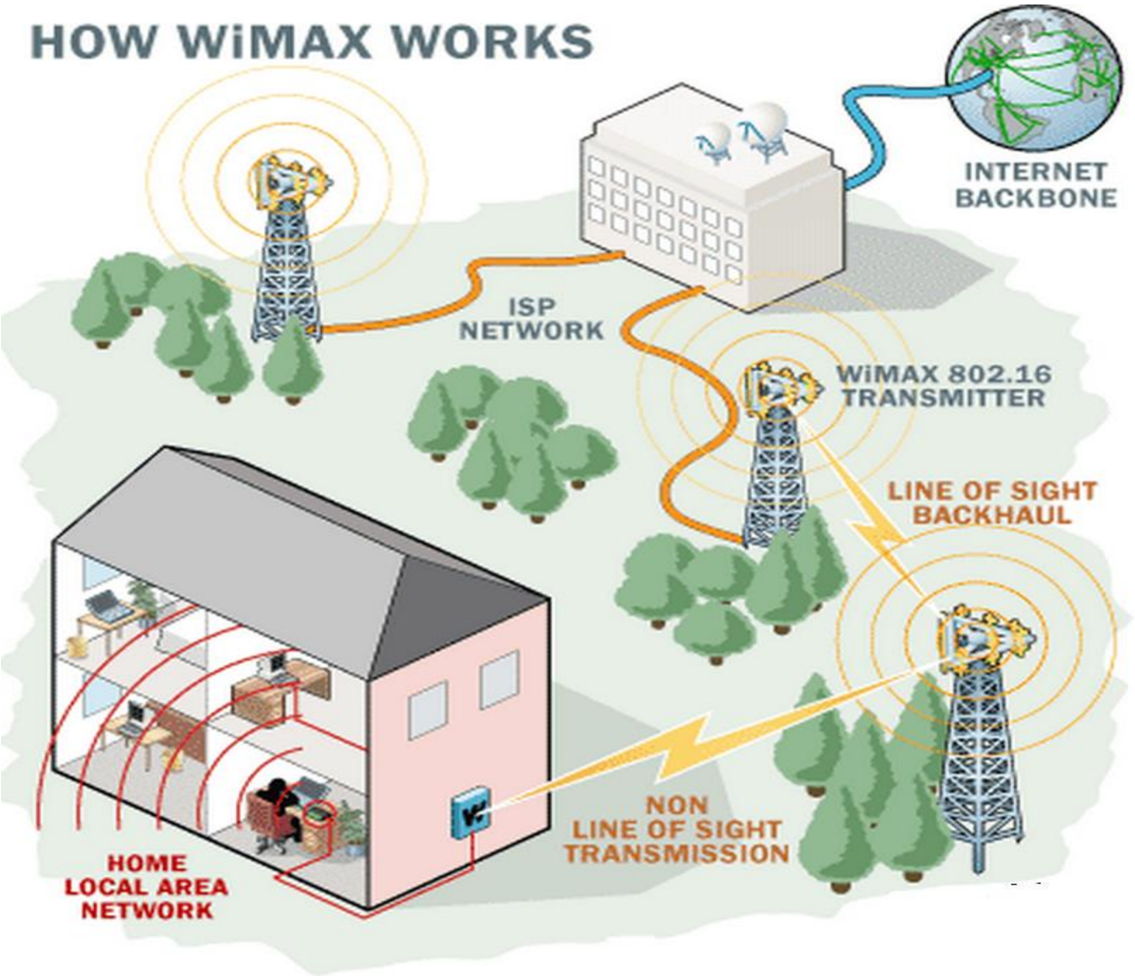


Figure 10. WiMAX connection Set-up (Howstuffworks, 2015).

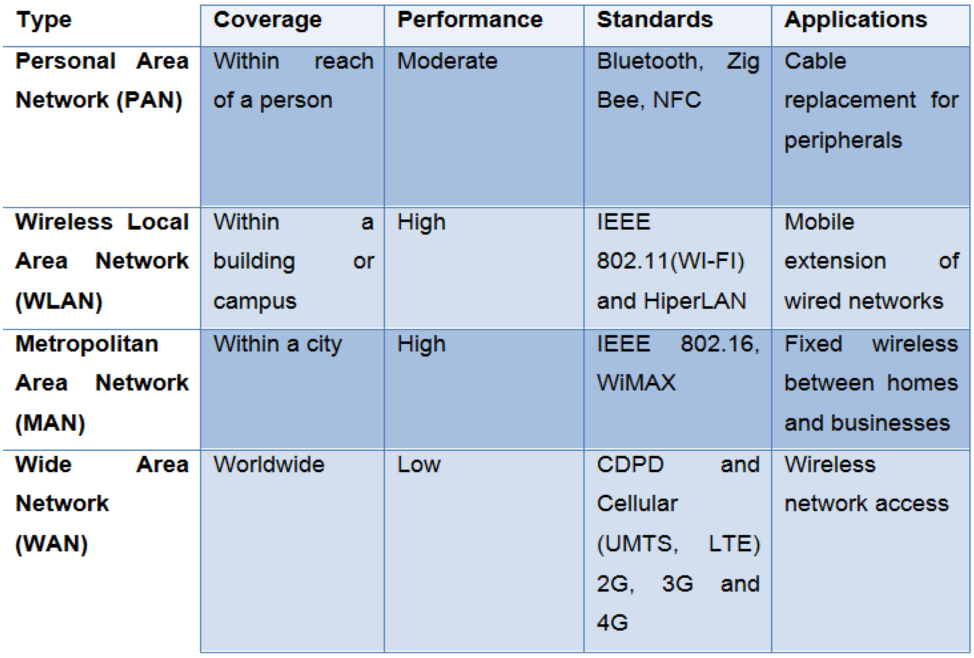
WiMAX provides two forms of wireless connection: a non-line of sight and a line of sight with frequencies range of 2 to 11GHz and 10 to 66GHz respectively.

6.4 WANs (Wide Area Networks)

Wide Area Networks types of networks cover a large geographical areas with the use of multiple satellite systems or satellite cables. These types of systems are referred to as 3G or 4G systems.

A cellular or mobile network is a wireless network distributed over land through cells where each cell includes a fixed location transceiver known as a cell site or base station.

Mobile network technology supports an orderly structure which is formed with the location registers, mobile switching center, public switched telephone network and base transceiver station. The base transceiver station enables cellular devices to make direct communication with mobile phones.



Type	Coverage	Performance	Standards	Applications
Personal Area Network (PAN)	Within reach of a person	Moderate	Bluetooth, Zig Bee, NFC	Cable replacement for peripherals
Wireless Local Area Network (WLAN)	Within a building or campus	High	IEEE 802.11(WI-FI) and HiperLAN	Mobile extension of wired networks
Metropolitan Area Network (MAN)	Within a city	High	IEEE 802.16, WiMAX	Fixed wireless between homes and businesses
Wide Area Network (WAN)	Worldwide	Low	CDPD and Cellular (UMTS, LTE) 2G, 3G and 4G	Wireless network access

Figure 11. Types of wireless networks.

7 WIRELESS NETWORK SECURITY

Wireless security is the prevention of unauthorized access or damage to computers and devices using wireless networks (Wikipedia, 2011b). They are two types of wireless security: wired equivalent privacy (WEP) and wi-fi protected access (WPA). A wireless network needs a multilayered approach to safeguard traffic, prevent hackers and unauthorized users.

This five-step approach is required to reduce the risks to wireless network (Cisco, 2014b):

1. Implement security policy.
2. Securing a WLAN.
3. Protecting a wired network from wireless attacks.
4. Protecting a network from outside attacks.
5. Setting-up a network security team.

7.1 Implement Security Policy

This policy is to secure and protect those who can use the network and how.

These are likely network security policies:

Acceptable use and Identity policy**:** This specifies who has access to the network by login details. It also signifies which network activities are allowed and which ones are not.

E-mail and communications Policy**:** This policy should ban or restrict the opening of unapproved or blocked websites and suspicious emails with attachments both from known and unknown contacts.

Antivirus policy: This policy install antivirus software and monitors it to protect the network from the Trojan horses, computer viruses and worms and similar viruses.

Password and Encryption policy: This policy implements a password change and content policy. The password should contains numbers, lower & upper case, symbol and users should be forced to change it every 90 days or regularly. The encryption policy is the use of algorithm or encryption technology to protect network data from unauthorised users.

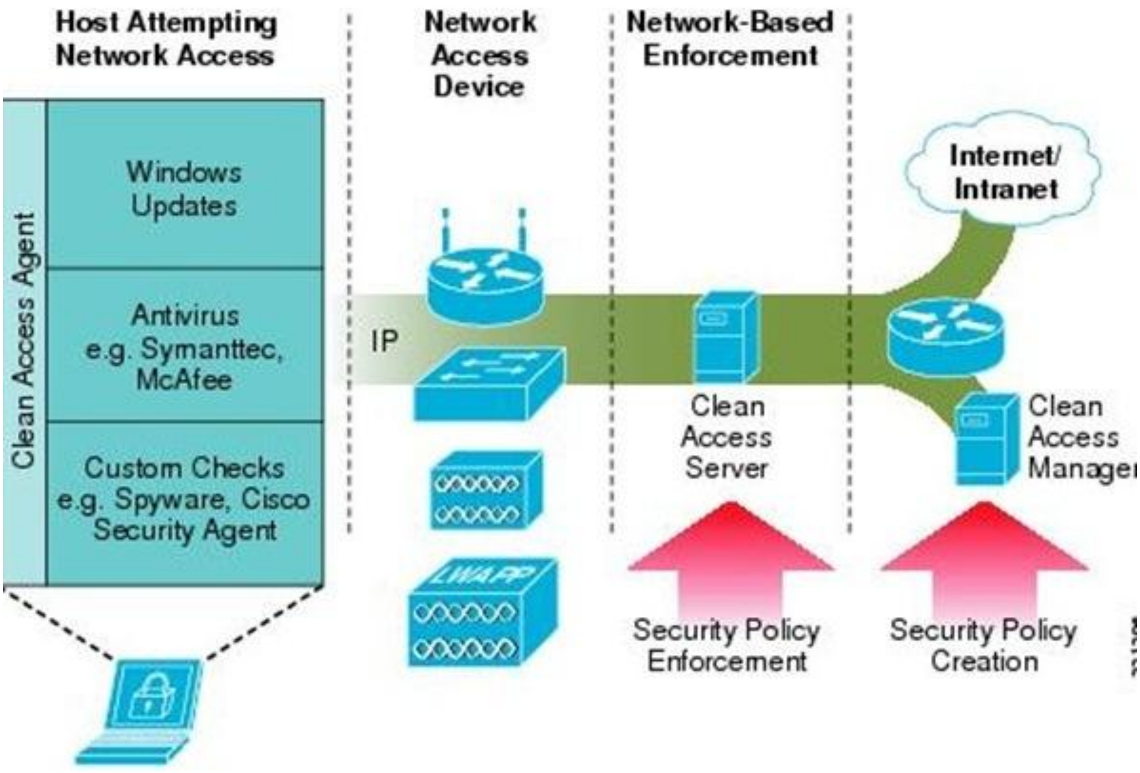

Host Attempting Network Access
Network Access Device
Network-Based Enforcement
Clean Access Agent
Windows Updates
Antivirus e.g. Symanttec, McAfee
Custom Checks e.g. Spyware, Cisco Security Agent
IP
LWAPP
Internet/ Intranet
Clean Access Server
Clean Access Manager
Security Policy Enforcement
Security Policy Creation

Figure 12. Wireless access and security measure (Cisco, 2014a).

7.2 Securing a WLAN

The following are some steps in securing a WLAN:

- Software updates
- Changing the default network name
- Encryption and Authentication: WPA2 is the best form of data encryption that can be used in wireless networks. It is the advanced encryption method which uses the advanced encryption standard (AES) to encrypt data for confidentiality and attack prevention.
- Adding VLANs or MAC address filters: A MAC address filter is maintained by the access points (APs) which permit only the MAC

address in the network to connect. VLAN control can also be implemented to restrict unauthorized users.

- Implementing Accessibility Barriers: Not all users should have access to all information. There should be a policy-based security approach for identity-based access. Users should only have access to the information that is needed to perform their job.
- Educating users and monitoring the network for malicious activities.

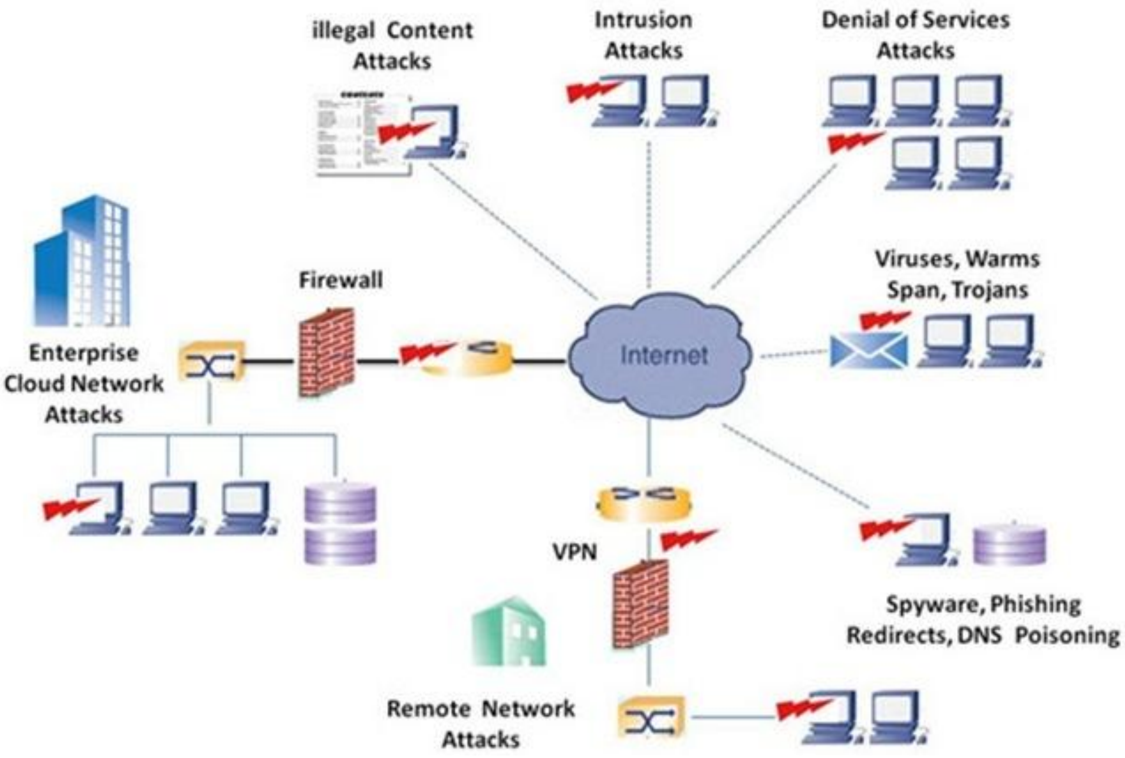

illegal Content Attacks
Intrusion Attacks
Denial of Services Attacks
Firewall
Viruses, Warms Span, Trojans
Enterprise Cloud Network Attacks
Internet
VPN
Spyware, Phishing Redirects, DNS Poisoning
Remote Network Attacks

Figure 13. Network Security Attack (Accton, 2014).

7.3 Protecting A Wired Network From Wireless Attacks

Installing wireless intelligent protection switching (IPS) devices will block unauthorized access and rogue traffic without affecting the network activities e.g., the use of Cisco Unified Wireless Network to monitor and prevent threats (Cisco, 2014b).

7.4 Protecting A Network from Outside Attacks

The use of anti-virus and anti-spyware software, firewalls, and VPNs protect wireless devices from outside attacks or threats. Cisco recommend the use of Cisco ASA 5500 which is an all-in-one device that can protect and safeguard the network with a secure VPN for encryption to protect network against data theft, firewall, protection of video and voice traffic, and IPS to filter malware from the network (Cisco, 2014b).

The use of Network Admission Control (NAC) appliance enables any devices connected to the network meets security standards.

7.5 Setting-up A Network Security Team

A security team's responsibilities are:

- To educate the users by giving information and training about passwords, privacy and passwords
- To give users access:
- To know the wireless coverage inside and outside the network area
- To monitor the network for any malicious activity. Deploying an intrusion protection system (IPS) and an intrusion detection system (IDS) helps to protect the network from suspicious activity.
- Must be aware of the latest hacking techniques.

CONCLUSION

The proposed approach in this thesis to improve wireless network dependability is based on design change and fault tolerance. These two approaches explain how to mitigate wireless network failure. Other aspects that affect wireless network dependability were also discussed.

The two approach discussed in this thesis can enhance the reliability of wireless and improve mobile networks, if the below attributes are to be considered:

- Characteristics of MTBF and MTTR
- Number of levels in the building block
- Number of customers supported

For future work, the two approaches can be developed with a simulation model. The simulation model will present some interesting aspects of the dependability attributes.

9 REFERENCES

Accton (2014), Network Security. Available at:

http://www.accton.com/Newspage.asp?sno=84 [Accessed 27 October 2014].

Al-Kuwaiti, M., Kyriakopoulos, N., Hussein, S., (2009) A Comparative Analysis of Network Dependability, Fault-tolerance, Reliability, Security, and Survivability. Communications Surveys & Tutorials, IEEE Volume:11, Issue: 2 pp 106 - 124 [Accessed 29 March 2014].

Cisco (2014a), Wireless NAC. Available at:

http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/secwlandg20/sw2dg/ch5_2_SPMb.html [Accessed 27 October 2014].

Cisco (2014b), Wireless Security. Available at:

http://www.cisco.com/web/solutions/smb/need_to/five_ways_to_improve_your_wireless_security.html [Accessed 10 September 2014].

Clublinks, 2015. Factors That Affect Wireless Speed and Reliability. Available at:

http://support.clublinks.com.au/support/articles/1000037385-factors-that-affect-wireless-speed-and-reliability [Accessed 31 January 2015]

Dazhi, C., and Pramod, K.V., (2004) QoS Support in Wireless Sensor Networks. Available at:

http://pdf.aminer.org/000/369/962/qos_support_in_wireless_sensor_networks_a_survey.pdf [Accessed 18 October 2014].

Hneiti, W., and Ajlouni, N., (2006) Dependability Analysis of Wireless Local Area Networks.

Information and Communication Technologies, ICTTA '06. 2nd, IEEE Volume:2

[Accessed 9 July 2014].

Howstuffworks (2015), WiMAX. Available at:

http://computer.howstuffworks.com/wimax1.htm [Accessed 20 January 2015].

Kharbash, S., and Wang, W., (2007) Computing Two-Terminal Reliability in Mobile Ad hoc Networks. Available at: http://www.ece.ncsu.edu/netwis/papers/07sw-wcnc.pdf [Accessed 15 October 2014].

Technopedia (2014a), WIMAX. Available at:

http://www.techopedia.com/definition/5102/worldwide-interoperability-for-microwave-access-wimax [Accessed 17 October 2014].

Varshney, U., and Malloy, A.D., (2001) Improving the dependability of wireless networks using design techniques. Local Computer Networks, 2001. Proceedings. LCN 2001. 26th IEEE Conference. [Accessed 29 March 2014].

Venkatesan, L., Shanmugavel, S., & Subramaniam, C., (2013) A Survey on Modeling and Enhancing Reliability of Wireless Sensor Network.

Wireless Network Sensor. Available at: http://file.scirp.org/Html/29346.html [Accessed 23 August 2014]

Wikipedia, (2014a) MTTF. Available at:

http://en.wikipedia.org/wiki/Mean_time_between_failures [Accessed 17 October 2014].

Wikipedia (2014b). Wireless Security. Available at:

http://en.wikipedia.org/wiki/Wireless_security [Accessed 10 September 2014].

Wikipedia (2015a), IEEE 802.11. Available at:

http://en.wikipedia.org/wiki/IEEE_802.11 [Accessed 20 January 2015].

4gon (2014) Wireless Performance. Available at:

http://www.4gon.co.uk/solutions/technical_factors_affecting_wireless_performance.php [Accessed 10 September 2014].