Wireless LAN Tutorial

Authors: Musadiq Umair

Dr. Kiramat Ullah

Abstract:

Wireless communication is the fast growing industry and will continue to evolve. A wireless local area network (WLAN) is a flexible data communications system that use radio frequency to transmit and receive information over the air instead of physical wires. Wireless connectivity allows free movement hence world has become increasingly mobile.

Introduction

Wireless networks have a great deal of flexibility, allows rapid deployment.

There are various typ of wireless networks such as BAN, PAN, WLAN, WiMax or cellular network etc., based on range. In cellular network, for example, base stations are used to connect users to an existing network as long as users remain within the range of the base station, they can take advantage of the network. A simple wired infrastructure connects to the Internet, and then the wireless network can accommodate as many users as needed.

WLAN is the type wil;ress network operatates in user space. IEEE 802.11std. is the first implemented WLAN standard operate in the 2.4 GHz frequency and has a maximum throughput of 1 to 2 Mbps. The improvements in standard over the years has improved its performance, widely used IEEE 802.11b still operates in the same frequency range, but with a maximum data rate of 11 Mbps.

1.1 **Architecture of Wireless LAN:**

Intro to WLAN (definition)

The basic service set (BSS), is a group of stations that communicate with each other in fuzzy area, called the basic service area, defined by the propagation characteristics of the wireless medium. Members of BSS can communicate in two manners:

1.1.1 *Independent BSS or Ad-Hoc Network:*

A BSS of stands alone devices communicate only peer to peer is called an Independent BSS or Ad-Hoc Network. There is no base to gives permission to talk. These networks are spontaneous and can be set up rapidly.

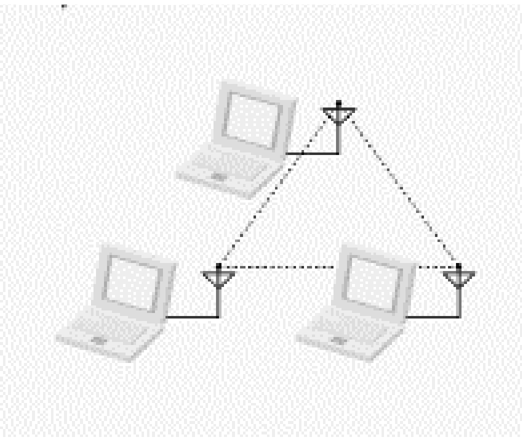

Figure 1-1: Independent BSS or Ad-Hoc

1.1.2 *Infrastructure BSS:*

Access points (APs) are used for communications of stations in infrastructure networks. All communication relay through APs, so takes at least two hops.

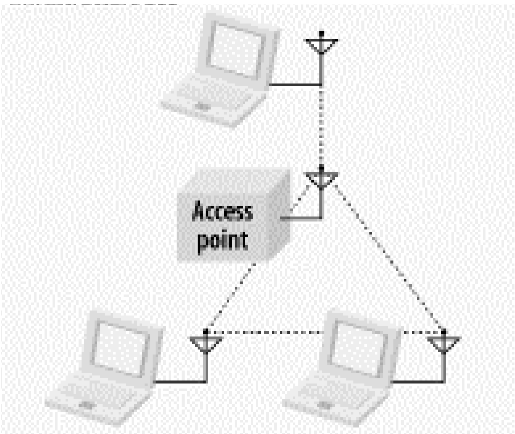

Figure 1-2: Infrastructure BSS

1.1.3 *Microcells and Roaming:*

The area of coverage for an access point is called a "microcell’. The installation of multiple access points is required in order to extend the WLAN range beyond the coverage of a single access.

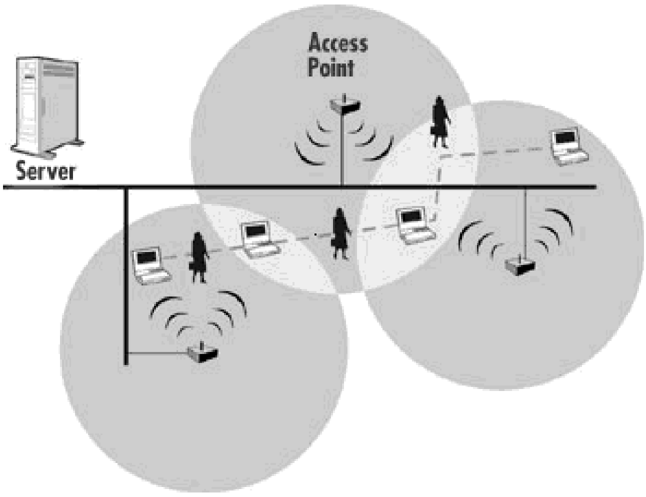

Figure 1-3: Microcells and Roaming

1.2 **WLAN Services:**

802.11 specify the services to be supported.

1.2.1 *Station Services (SS)*

Authentication:

To control network access, stations first establish their identities. Stations have to prove identity by passing a series of tests before acknowledged and allowed to converse. The authentication is relationship between two stations inside an IBSS or to the AP of the BSS. Once authenticated, it may then associate itself. There are two types of authentication services offered by 802.11.

Open-System Authentication:

One tries to authenticate will receive authentication.

Shared Key Authentication:

The users must possess a shared key. The shared secret is implemented with the use of the Wired Equivalent Privacy (WEP) privacy algorithm. The shared secret is securely delivered to all stations ahead of time.

De-authentication:

The station or AP desire to terminate a stations authentication, the station is automatically disassociated.

Privacy

An encryption algorithm is used to avoid eavesdropping on your LAN traffic. Wired Equivalent Privacy (WEP) is an optional algorithm to satisfy privacy. All stations start encryption mode until they are authenticated.

MAC Service Data Unit (MSDU) Delivery

MSDU delivery ensures that the information is delivered between the medium access control service access points.

1.2.2 *Distribution System Services (DSS).*

Association

A station has to affiliate itself to BSS infrastructure when it wants to use the LAN. This is done by associating itself with an access point. Associations are dynamic in nature as stations can move, turn on or off. A station can only be associated with one AP.

Re-association

Association supports no-transition mobility that is not enough to support BSS-transition. Re-association service allows the station to switch its association from one AP to another. Both association and re-association are initiated by the station.

Disassociation

Disassociation is when the association between the station and the AP is terminated. This can be initiated by either party. A disassociated station cannot send or receive data. A station that move to a new Extended Service Station will have to reinitiate connections.

Distribution

Obtain data from the sender to the intended receiver. The message is sent to the local AP (input AP), then distributed through the Distributed System to the AP (output AP) that the recipient is associated with. If the sender and receiver are in the same BSS, the input and out AP's are the same. So distribution service is logically invoked whether the data is going through the DS or not.

Integration

Integration is when the output AP is a portal. Thus, 802.x LANs are integrated into the 802.11 DS.

1.3 WLAN Advantages

There are several features of wireless LAN:

Simplicity: Wireless communication system are easy and fast to deploy in comparison of cabled network. Initial setup cost could be a bit high but other advantages overcome that high cost.

Reachability: In what concern the end user connectivity, WOLAN allaows connectivity to wireless communication systems (tcp/ip or ninternet), enable people to be stay connected and be reachable, regardless of the location they are operating from.

Mobility: Provide mobile users with access to real-time information so that they can roam around in the network without getting disconnected from the network. Users can move seamlessly between access points without having to log in again and restart their applications

Flexibility: Wireless networks offer more flexibility and adapt easily to changes in the configuration of the network.

Handed off: Access points have a way of exchanging information as a user connection is handed off from one access point to another, wireless nodes and access points frequently check the strength and quality of transmission

Scalability: wireless systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations can be easily changed and range from peer-to-peer networks suitable for a small number of users to large infrastructure networks that enable roaming over a broad area.

1.4 **Issues of WLAN**

There are following issues with Wireless Networks.

1.4.1 ***Quality of Service (QoS):***

One of the primary concerns about wireless data delivery is that, unlike the Internet through wired services, QoS is inadequate. Lost packets and atmospheric interference are recurring problems of the wireless protocols.

- For application where mobility not required a wired connection provide a faster, reliable and cost-effective solution.

- Higher loss-rates due to interference (due to other communcaiotnsd)

- Restrictive regulations of frequencies (e.g., wlan operates in ISM is unlicend specprm which has huge deployment)

- Wireless network technology has low data throughput and data transmission rates due to collisions

- Higher latency, higher jitter due to channel access.

- Wireless technology does not provide the same bandwidth guarantees as a wired connection and is additionally shared with other users who are connected to the same access point.

- Wireless networks are subject to interference from any electromagnetic sources

- The signal strength is greatly reduced by obstacles.

- Congestion problems or even failure under error conditions or high or malicious traffic, the actions of a few can potentially affect the network connections of many.

- Limited channel selection induces “co-channel interference”. This interference happens when the access points are stepping on each other and is harmful to the performance of your network.

1.4.2 ***Security Risk:***

A data transfer over a wireless network. Basic network security mechanisms like the service set identifier (SSID) and Wireless Equivalency Privacy (WEP); these measures may be adequate for residences and small businesses, but they are inadequate for the entities that require stronger security.

- **Denial of Service:**

  The intruder floods network with valid or invalid messages affecting the availability of the network resources. The low bit rates of WLAN can be exploit to leave them open to denial of service attacks. Radio interference can be used to unable WLAN to communicate.

- **Spoofing and Session Hijacking:**

  The attacker may gain access to privileged data and resources in the network by using identity of a valid user. Attackers spoof MAC addresses, and act as illegitimate AP. To avoid spoofing, authentication and access control mechanisms need to be placed in the WLAN.

- **Eavesdropping:**

  Eavesdropping is the most significant threat because the attacker can intercept the transmission, as it is impossible to control who can receive the signals in wireless LAN as medium is shared.

1.5 Motivation:

Due to shared and broadcast medium and overhearinfg, the wireless nodes are exposed to attacks. Security is one of the major drawbsack in wilress network as compared to wired one. Risks involve various attacks whicb causing deassociations, interferenmce, ande/or co0llisons etc,. As a result we faces delay and loss of data.

In order to take full advanagtwed pf WLAN dfacilities, we need to address the isuuses such as attcks, by enahcguing QoS.

In this thesis we auim to uibnvesigae

1.5 Scope

Move to intro if necessary

1.5 ***Solutions of WLAN issues:***

1.5.1 ***Use of infrastructure BSS:***

As Ad-Hoc networks have issues to control traffic in network, these can be overcome by use of Access Points (APs). Although the multi hop transmission takes more transmission capacity than a directed frame from the sender to the receiver, it has two major advantages:

- *All stations should be in range of the AP, no restriction placed on distance between mobile stations themselves. Direct communication between mobile stations can save transmission capacity but increases physical layer complexity because mobile stations would need to maintain neighbor relationships with all other mobile stations within the service area.*
- *Access points can assist stations attempting to save power. AP can note when a station enters a power-saving mode and buffer frames for it. Battery-operated stations can turn the wireless transceiver off and power it up only to transmit and retrieve buffered frames from the access point.*

References

1. M. Naeem, Jorge Diaz-Martinez, Shariq Aziz Butt and Nicolo Montesano, “Trends and Future Perspective Challenges in Big Data”, in Proc. Of The Sixth Euro-China Conference on Intelligent Data Analysis and Applications (ECC2019) Arad-Romania, March 2020.
2. Z. Haider and M. Saleem,"Analysis of Interference in Wireless", in Proc. of ArXiv, arXiv:1810.13164 [cs.NI], Oct. 2018.
3. A Khalid, SA Butt, and S Gochhait, “Agile Scrum Issues at Large-Scale Distributed Projects: Scrum Project Development At Large”, in International Journal of Software Innovation (IJSI), Vol 8, Issue 2, Pages: 85-94, IGI Global 2020.
4. S Gochhait, SA Butt, and A Ali, “Cloud Enhances Agile Software Development” Book Chapter in Cloud Computing Applications and Techniques for E -Commerce, Pages: 28-49, IGI Global, 2020.
5. M Alam, and MM Umair, "Detection and Prevention Against RTS Attacks in Wireless LANs", in Proc. of IEEE C-CODE, Islamabad Pakistan, Mar. 2017.
6. T. Jamal, and SA Butt, "Malicious Node Analysis in MANETS", in Proc. of International Journal of Information Technology, PP. 1-9, Springer Publisher, Apr. 2018.
7. S. A. Butt, and M. Shoaib, "IoT Smart Health Security Threats," in proc. of 19th International Conference on Computational Science and Its Applications (ICCSA), Saint Petersburg, Russia, 2019, pp. 26- 31. doi: 10.1109/ICCSA.2019.000-8.
8. M. Asam and Z. Haider, "Security Issues in WBANs", in proc. of Arxiv, Volume arXiv:1911.04330 [cs.NI], November 2019.
9. M. Asam and Z. Haider, "Novel Relay Selection Protocol for Cooperative Networks", in proc. of Arxiv, Volume arXiv: 1911.07764 [cs.NI], November 2019.
10. Zeeshan Haider, Muhammad Asam, Shariq Butt and Aleena Ajaz, "Mitigation of Wireless Body Area Networks Challenges using Cooperation", International Journal of Security and Its Applications (IJSIA), ISSN: 1738-9976(Print); 2207-9629(Online), NADIA, (2020), Vol. 14, No. 1, pp. 15-30.
11. SA Butt and M. Ajmal Azad, "A multivariant secure framework for smart mobile health application", in Transactions on Emerging Telecommunications Technologies, Aug. 2019.
12. M. Asam and A. Ajaz, “Challenges in Wireless Body Area Network”, in Proc. of International Journal of Advanced Computer Science and Applications, Volume 10, No. 11, Nov. 2019.
13. SA Butt and A. Ali, "Predictive Variables for Agile Development Merging Cloud Computing Services", in Proc. of IEEE Access, Volume 7, 2019. DOI: 10.1109/ACCESS.2019.2929169.
14. P. Mendes, “Analysis of Hybrid Relaying in Cooperative WLAN”, In Proc. of IEEE IFIP Wireless Days (WD), Valencia, Spain, November 2013.
15. P. Mendes, and A. Zúquete, “Relayspot: A Framework for Opportunistic Cooperative Relaying”, in Proc. of IARIA ACCESS, Luxembourg, June 2011.
16. SA Butt, “Cooperative Cloudlet for Pervasive Networks”, in Proc. of Asia Pacific Journal of Multidisciplinary Research, Vol. 5, No. 3, PP. 42-26, Aug 2017.
17. SA Butt, and T. Jamal, “Frequent Change Request from User to Handle Cost on Project in Agile Model”, in Proc. of Asia Pacific Journal of Multidisciplinary Research 5 (2), 26-42, 2017.

18. P. Amaral, “Flow Table Congestion in Software Defined Networks”, in Proc. of IARIA 12th ICDS, Rome Italy, Mar. 2018.
19. P. Mendes, and A. Zúquete, “Wireless Cooperative Relaying Based on Opportunistic Relay Selection”, in Proc. of International Journal on Advances in Networks and Services, Vol. 5, No. 2, PP. 116-127, Jun. 2012.
20. SA Butt, and T. Jamal, “Study of Black Hole Attack in AODV”, in Proc. of International Journal of Future Generation Communication and Networking, Vol. 10, No.9, pp. 37-48, 2017.
21. SA Butt, “Low-Energy Adaptive Clustering Hierarchy (LEACH) Enhancement for Military Security Operations”, In Proc. Of Journal of Basic and Applied Scientific Research, ISSN 2090-4304, 2017.
22. Z. Haider, "Denial of Service Attack in Cooperative Networks", in Proc. of ArXiv, arXiv: CoRR Vol. arXiv:1810.11070 [cs.NI], Oct. 2018.
23. T. Jamal and P. Mendes, “Relay Selection Approaches for Wireless Cooperative Networks”, in Proc. of IEEE WiMob, Niagara Falls, Canada, Oct. 2010.
24. T. Jamal and P. Mendes, “Cooperative relaying in user-centric networking under interference conditions”, in Proc. of IEEE Communications Magazine, vol. 52, no. 12, pp. 18–24, Dec 2014.
25. Fawad, U., et al. "Proton, UV, and X-ray Induced Luminescence in [Tb.sup.3+] Doped Lu[Gd.sub.2][Ga.sub.2][Al.sub.3][O.sub.12] Phosphors." Crystals, vol. 10, no. 9, 2020.
26. Fawad, U.; Kim, H. J.; Gul, Ibrahim; Khan, Matiullah; Tahir, Sajjad; Jamal, Tauseef; Muhammad, Wazir. 2020. "Proton, UV, and X-ray Induced Luminescence in Tb3+ Doped LuGd2Ga2Al3O12 Phosphors" *Crystals* 10, no. 9: 844.
27. T. Jama, and A. Zúquete, “Opportunistic Relay Selection for Wireless Cooperative Network”, in Proc. of IEEE IFIP NTMS, Istanbul Turkey, May 2012.
28. P. Mendes, W. Moreira and Huiling Zhu, “Cooperative Networking in User-Centric Wireless Networks”, In: Aldini A., Bogliolo A. (eds) User-Centric Networking. Lecture Notes in Social Networks. Springer, Cham, ISBN 978-3-319- 05217-5, May 2014.
29. T. Jamal, and P. Mendes, “COOPERATIVE RELAYING FOR DYNAMIC NETWORKS”, EU PATENT, (EP13182366.8), Aug. 2013.
30. T. Jamal, and P. Mendes, “802.11 Medium Access Control In MiXiM”, in Proc. of Tech Rep. SITILabs-TR-13-02, University Lusófona, Lisbon Portugal, Mar. 2013.
31. L. Lopes, T. Jamal, and P. Mendes, "Towards Implementing Cooperative Relaying", In Proc. of Technical Report COPE-TR-13-06, CopeLabs University Lusofona Portugal, Jan 2013.

32. P. Mendes, and A. Zúquete, “Interference-Aware Opportunistic Relay Selection”, In Proc. of ACM CoNEXT student workshop, Tokyo, Japan, Dec. 2011.
33. T. Jamal, "Cooperative MAC for Wireless Network", In Proc. of 1st MAP Tele Workshop, Porto, Portugal, 2010.
34. T. Jamal, and P. Mendes, “Cooperative Relaying for Wireless Local Area Networks”, In: Ganchev I., Curado M., Kassler A. (eds) Wireless Networking for Moving Objects. Lecture Notes in Computer Science, vol 8611. Springer, Cham, (WiNeMo), Aug. 2014.
35. R. Sofia, P. Mendes, W. Moreira, A. Ribeiro, S. Queiroz, A. Junior, T. Jamal, N. Chama, and L. Carvalho, “Upns: User Provided Networks, technical report: Living-Examples, Challenges, Advantages”, Tech. Rep. SITI-TR-11- 03, Research Unit in Informatics Systems and Technologies (SITI), University Lusofona, Lisbon Portugal, Mar. 2011.
36. P. Mendes, “Cooperative Relaying in Wireless User-Centric Networks”, Book Chapter In: Aldini, A., Bogliolo, A. (eds.) User Centric Networking. Lecture Notes in Social Networks, Springer, Cham, pp. 171–195, 2014.
37. T. Jamal, P. Mendes, and A. Zúquete, “Design and Performance of Wireless Cooperative Relaying”, PhD Thesis MAP-Tele, University of Aveiro, Oct. 2013.
38. T. Jamal, P. Mendes, and A. Zuquete, “RelaySpot: Cooperative Wireless Relaying”, in Proc. of MAP-Tele Workshop, Aveiro, Portugal, May 2011.
39. T. Jamal, and P. Mendes, “Cooperative Wireless Relaying, Key Factors for Relay Selection”, in Proc. of MAP-Tele Workshop, Porto, Portugal, Dec. 2009.
40. T. Jamal, and P. Mendes, “RelaySpot, OMNET++ Module”, Software Simulator Extension In Proc. of COPE-SW-13-05, 2013.
41. P Amaral, A Khan, SAB, Kiramat, "Denial of Service Attack in Wireless LAN", in Proc of 12th ICDS 2018, Rome Italy.