WLAN Tutorial

Dr. Abbas Khurum
Pakistan Institute of Engineering and Applied Sciences (PIEAS)

***Abstract*— WLAN is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communications. Maintained by the Institute of Electrical and Electronics Engineers (IEEE) LAN/MAN Standards Committee (IEEE 802). This document highlights the main features of IEEE 802.11n variant such as MIMO, frame aggregation and beamforming along with the problems in this variant and their solutions**

Keywords—Wireless Local Area Network (WLAN), Local Area Network (LAN), Multiple Input Multiple Output (MIMO), frame aggregation, beamforming, Denial of Service (DOS), fairness

I. INTRODUCTION

IEEE LAN/MAN standards committee develops and maintains networking standards, recommended practices and guides for local, metropolitan and other area networks, using an open and accredited process. IEEE 802.11 has set of rules required to establish and implement a wireless network. The variant discussed in this report is 802.11n. The goal of the 802.11n standard is to significantly increase throughput (Throughput is a measure of how many units of information a system can process in a given amount of time). The baseline goal of the standard was to reach speeds of 100Mbps. Given the right conditions, the theoretical speeds of 802.11n are estimated to reach a staggering 450Mbps. In practical operations, 802.11n speeds will be much slower.

Some of the features of 802.11n are as follows:

II. FEATURES of 802.11N

A. MIMO

Multiple Input Multiple Output (MIMO) is a method to increase data rates and improve networks throughput. It does so by using multiple antennas of which some are used for sending data frames and some for receiving data frames. Using multiple antennas helps in avoiding collisions and interferences.

Figure 1. Multiple Input Multiple Output device

B. Frame Aggregation

Frame aggregation is a feature in WLAN standards that increases throughput by sending two or more data frames in a single transmission. By grouping several frames into one large frame and since management information needs to be specified only once per frame, the ratio of payload data to total volume of data is higher, allowing higher throughput.

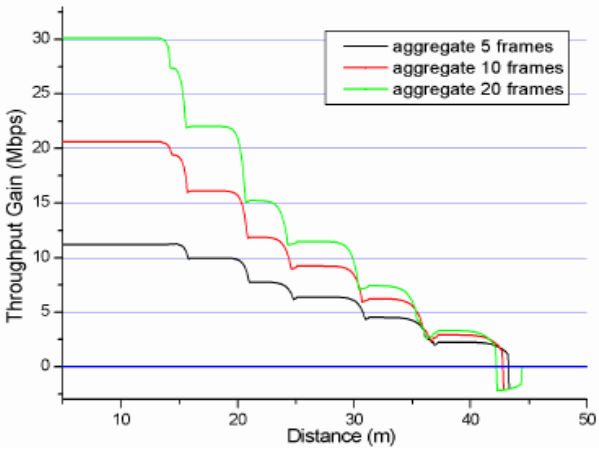

Figure 2. Increase in throughput gain in single transmission

C. Beamforming

It is a signal processing technique in which the router improves the signal strength specifically in the direction of the client device. It is achieved by combining elements in an antenna array in such a way that signals at particular angels experience constructive interferences while others experience destructive interferences.

Figure 3. Improves signal strength

III. PROBLEMS

Security Risks due to wireless medium as any connected user to the same router can initiate DOS attacks, eavesdropping, and man in the middle attacks. Clients that form unauthorized connections of any type, whether accidentally or intentionally, put themselves and corporate data at risk. Some enterprise use Group Policy Objects to configure authorized connections and prevent end-user changes. Others use host-resident agents and/or WIPS to monitor client activity and disconnect high- risk connections. Some clients leak the data from network. Some client/end user/router may allow unauthorized client to connect in network. Attackers have refocused their attention on endpoints. Numerous exploits have been published to take advantage of buggy drivers, using buffer overflows to execute arbitrary commands and became part of network. Wireless LANs are easy to find. Security risks are due to:

1.1 Easy Access

- All wireless networks need to announce their existence
- The information needed to join a network is also the information needed to launch an attack on a network.

- Your 802.11 network and its parameters are available for anybody with a Wi-Fi device.
- Short of moving into heavily shielded offices pace that does not allow RF signals to escape, there is no solution for this problem.

1.2 "Rogue" Access Points

- Easy access to wireless LANs is coupled with easy deployment.
- Any user can run to a nearby computer store, purchase an access point and connect it to the corporate network without authorization.

1.3 Connectivity

- Suffers from the issue of fairness among receivers
- Suffers from interferences from other appliances as devices such as microwaves emits signals in the 2.4GHz bandwidth

IV. SOLUTIONS

Improved security on router level to be able to detect malicious user and reject further connectivity. Encryption on data packets so that no eavesdropping on data stealing can be done via asymmetric cryptography. At the sender the checksum of the message (which is the unencrypted data that needs to be transmitted) is calculated and the result is concatenated to the end of it. A key stream should be generated. A secret key that is agreed upon by the hosts and servers of the network and is hard coded in them during the original set up of the network. Usually this key does not change for long time, sometimes as long as the life of the network. Other improvements is making the secret key dynamic so before the attacker has enough time to gather information to break the key, the key is changed. This is also a significant improvement since the original static key implementation was inherently vulnerable.

Fairness for users can be improved by Enhanced Distributed Coordination Access (EDCA) that prioritized quality of service and using reduced inter-frame space (RIFS).

Interferences can be reduced by broadcasting on 2.4GHz and 5GHz simultaneously. It is also increases client capacity as users can be accommodated on both hands. Since users are divided on separate bandwidths, the overall performance improves for users.

V. CONCLUSION

IEEE 802.11n has come up as a way to solve many of the issues presented in previous variants of 802.11. Improving on networking speeds and overall throughput that are especially beneficial for single antenna devices like smartphones, as Wi-Fi connection has to remain active for less period of time because data transferring takes less amount of time. However, like every wireless network it has its weaknesses due to characteristics of a wireless medium. The above-mentioned solutions for problems can help in reducing attacks on the network making it safer as authentication during initial connectivity has been strengthened.

REFERENCES

[1] Z. Haider, M. Saleem, and T. Jamal, "Analysis of Interference in Wireless", in Proc. of ArXiv, arXiv:1810.13164 [cs.NI], Oct. 2018.

[2] T. Jamal and P. Mendes, "Relay Selection Approaches for Wireless Cooperative Networks", in Proc. of IEEE WiMob, Niagara Falls, Canada, Oct. 2010.

[3] T. Jamal, P. Mendes, and A. Zúquete, “Opportunistic Relay Selection for Wireless Cooperative Network”, in Proc. of IEEE IFIP NTMS, Istanbul Turkey, May 2012.
[4] 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.
[5] P. Mendes, W. Moreira, T. Jamal, 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.
[6] T. Jamal, P. Mendes, and A. Zúquete, “Relayspot: A Framework for Opportunistic Cooperative Relaying”, in Proc. of IARIA ACCESS, Luxembourg, June 2011.
[7] 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.
[8] T. Jamal, M Alam, and MM Umair, "Detection and Prevention Against RTS Attacks in Wireless LANs", in Proc. of IEEE C-CODE, Islamabad Pakistan, Mar. 2017.
[9] T. Jamal, P. Mendes, and A. Zúquete, “Interference-Aware Opportunistic Relay Selection”, In Proc. of ACM CoNEXT student workshop, Tokyo, Japan, Dec. 2011.
[10] T. Jamal and P. Mendes, “Analysis of Hybrid Relaying in Cooperative WLAN”, In Proc. of IEEE IFIP Wireless Days (WD), Valencia, Spain, November 2013.
[11] 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.
[12] T. Jamal, and 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.
[13] T. Jamal, 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.
[14] 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.
[15] T. Jamal, and P. Amaral, “Flow Table Congestion in Software Defined Networks”, in Proc. of IARIA 12th ICDS, Rome Italy, Mar. 2018.
[16] T. Jamal, and 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.
[17] 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.
[18] T. Jamal, and 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.
[19] T. Jamal and Z. Haider, "Denial of Service Attack in Cooperative Networks", in Proc. of ArXiv, arXiv: CoRR Vol. arXiv:1810.11070 [cs.NI], Oct. 2018.
[20] Z. Haider, K. Ullah and T. Jamal, "DoS Attacks at Cooperative MAC", in Proc. of ArXiv, arXiv:1812.04935 [cs.NI], Dec. 2018.