CPU and Memory Utilization

The average CPU utilization by the Master and Slave Access Points is illustrated in Table 3.

Table -3: CPU and Memory usage by Access Points

Node Type	*CPU*	*Memory*	*AP Reset*
Master	34%	63%	No
Slave	57%	45%	No

The CPU and memory utilization are considerably good which is measured for a period of 24 hours. As seen in table 3, the Access points do not reboot or move into the unstable mode. Hence the stability of the kernel remains stable without any network interruption. From the above table inference, the proposed P2P model yields better results than the existing Mesh mode.

V. CONCLUSION & FUTURE SCOPE

Using the existing Wi-Fi Mesh model an enhanced P2P Mesh Wi-Fi model is proposed using the Master-Slave approach, for overcoming the drawbacks of Mesh network Wi-Fi model. This work has successfully recognized and classified the difference in various factors i.e. Dynamic frequency selection, dynamic Peering, Bandwidth, Frequency etc. Also, the effectiveness of the Algorithms like SAE, AMPE, HWMP on the P2P was tested. Results prove that the P2P model can be used in outdoor applications which has the necessity of increased range. The Antenna integrated in the outdoor Access point is 4x4, has been used to increase the link rate, gain and directivity. The U-NII 2 and U-NII 2 extended bandwidth spectrum for more number of Bandwidth channel allocation which enhances the Dynamic healing capability and scalability.

The proposed model can be enhanced further by employing CSMA-CA timers at the Master and Slave Access Points. This focuses on Automatic Distance locating of Access Points, suitable for high Bandwidth, Data rate and range applications. The Directivity and Gain of the antenna can be increased by deploying LED in the Antenna hardware of the Access point, which in turn increases the throughput factor.

REFERENCES

[1]. G. Debita and K. Staniec, "Methodology of the Wireless Networks Planning in Mesh Topology," 2008 Third International Conference on Dependability of Computer Systems DepCoS-RELCOMEX, Szklarska Poreba, 2008, pp.375-382,doi: 10.1109/DepCoS-RELCOMEX.2008.61.

[2]. S. Y. Shahdad, A. Sabahath and R. Parveez, "Architecture, issues and challenges of wireless mesh network," 2016 International Conference on Communication and Signal Processing (ICCSP), Melmaruvathur, 2016, pp. 0557-0560, doi: 10.1109/ICCSP.2016.7754201.

[3]. Wang, Xudong & Lim, Azman. (2008). IEEE 802.11s wireless mesh networks: Framework and challenges. AdHoc Networks. 6. 970-984. 10.1016/j.adhoc.2007.09.003.

[4]. A. K. Roy and A. Kumar Khan, "Performance Degradation in Wireless Mesh Networks via External and Internal Attacks," 2019 2nd International Conference on Innovations in Electronics, Signal Processing and Communication (IESC), Shillong, India,2019, pp.258-262, doi: 10.1109/IESPC.2019.8902374.

[5]. Roy, Amit Kumar and Khan, Ajoy Kumar, Architectural and Security Perspective of Wireless Mesh Network (March 19, 2019). International Journal of Computational Intelligence & IoT, Vol. 2, No. 1, 2019.

[6]. K. K. Thangadorai, K. Murugesan, V. B. Joseph and D. Das, "A Novel Process to Avoid Redundant Encryption and Decryption in Wi-Fi Mesh Network," *2018 IEEE* International Conference on Electronics, Computing and Communication Technologies (CONECCT), Bangalore,2018, pp.1-6, doi: 10.1109/CONECCT.2018.8482377.

[7]. D. Harkins, "Simultaneous Authentication of Equals: A Secure, Password-Based Key Exchange for Mesh Networks," 2008 Second International Conference on Sensor Technologies andApplications (sensorcomm 2008), Cap Esterel, 2008, pp. 839-844, doi: 10.1109/SENSORCOMM.2008.131.

[8]. G. R. Hiertz et al., "IEEE 802.11s: The WLAN Mesh Standard," in IEEE Wireless Communications, vol. 17, no. 1, pp. 104-111, February 2010, doi: 10.1109/MWC.2010.5416357.

[9]. M. Filho, M. Ribeiro, I. Silva, A. Santos, C. Oliveira and R. Braga, "Performance Issues in a Low-Cost Multi-Channel Multi-Interface Wireless Mesh Network," 2018 IEEE Symposium on Computers and Communications (ISCC), Natal, 2018, pp. 00792-00795, doi: 10.1109/ISCC.2018.8538458.

[10]. L in, C., Shieh, C., Hwang, W. et al. Proportional b andwidth allocation with consideration of delay c onstraint over IEEE 802.11e-based wireless mesh n etworks. Wireless Netw 24, 1575–1592 (2018).

[11]. P. Karimi, W. Lehr, I. Seskar and D. Raychaudhuri, "SMAP: A Scalable and Distributed Architecture for Dynamic Spectrum Management," 2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Seoul, 2018, pp. 1-10, doi: 10.1109/DySPAN.2018.8610416.

[12]. B. He, S. Joshi, D. P. Agrawal and D. Sun, "An Efficient Authenticated Key Establishment Scheme for Wireless Mesh Networks," 2010 IEEE Global

Telecommunications Conference GLOBECOM 2010, Miami, FL, 2010, pp. 1-5, doi: 10.1109/GLOCOM.2010.5683733.

[13]. P. Subhash and S. Ramachandram, "Secure neighbour discovery in wireless mesh networks using connectivity information," 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Kochi, 2015, pp. 2061-2066, doi: 10.1109/ICACCI.2015.7275920.

[14]. S. M. S. Bari, F. Anwar and M. H. Masud, "Performance study of hybrid Wireless Mesh Protocol (HWMP) for IEEE 802.11s WLAN mesh networks," 2012 International Conference on Computer and Communication Engineering (ICCCE), Kuala Lumpur, 2012, pp.712-716, doi: 10.1109/ICCCE.2012.6271309.

[15]. Ming Ann Ng and K. A. Yau, "An energy-efficient Hybrid Wireless Mesh Protocol (HWMP) for IEEE 802.11s mesh networks," 2013 IEEE International Conference on Control System, Computing and Engineering, Mindeb, 2013, pp. 17-21, doi: 10.1109/ICCSCE.2013.6719925.