Congestion Based Adaptive Association Mechanism for IEEE 802.11ah Based Large IoT Network

Nandhini R and Radha R(✉)

School of Computer Science and Engineering, Vellore Institute of Technology–Chennai, Chennai, India
radhu.mithu@gmail.com

Abstract. The IEEE 802.11 ah standard is the prominent protocol for medium range communication in the domain of Internet of Things (IoT), facilitating interaction between wireless sensor nodes and access points. Supporting up to approximately 8192 nodes connected to a single access point through single hop strategies, IEEE 802.11 ah employs CSMA/CA for the authentication and association process of sensor nodes with access point. However, the standard encounters challenges such as significant collisions and prolonged network setup times when attempting to associate an excessive number of wireless sensor nodes with a single access point, primarily due to authentication thresholds set at intervals. In this research, we propose a dynamic adjustment of the authentication threshold based on network congestion status. Learning parameters including the number of requests served successfully by the access point in the past, present and a congestion threshold are leveraged to adapt to current network congestion levels. Through evaluation using the LILD method in the ns-3 simulator, our approach demonstrates considerable enhancements in terms of collision reduction and network setup efficiency. This research endeavours to promote responsible network management practices for improving the performance and reliability of IEEE 802.11 ah based IoT deployments.

Keywords: Wi-Fi Halow · IoT · Association Process · Mitigate Congestion

1 Introduction

The Internet of Things (IoT) is a network of interconnected devices equipped with software & other technologies that allow them to collect, store and exchange data with other devices and systems. These devices includes everyday household appliances and wearables to industrial related machinery and vehicles. A bibliometric study was conducted over the Internet of Things (IoT) from 2000 to 2019, using co-citation, coupling, and cluster analysis methods to evaluate the development and research trends of the IoT, from which the main thematic trends,

P. Pareek et al. (Eds.): IC4S 2024, LNICST 599, pp. 363–377, 2025.
https://doi.org/10.1007/978-3-031-77081-4_29

collaboration networks, and challenges of IoT development are incurred. It also gives valuable insights for researchers, entrepreneurs, and governments to understand the development of the IoT over the past 20 years and in It identifies key research topics such as IoT security, wireless sensor networks, IoT management, and privacy. Security and algorithm issues have become basic themes in recent years. [1].

A comprehensive overview of the Internet of Things (IoT) provides the study of architectures, protocols, applications and detailed description about recent advancements, future directions, and recommendations, and also gives insights into spread spectrum techniques, IoT middleware, simulators, research history, and emerging challenges. Gives a brief note on about the evolution of IoT and about the protocols, technologies, applications, and the research challenges that exists when implementing it. Additionally, it addresses mobility management, maintenance costs, internet disconnection issues, and security challenges in IoT environments. [2].

Internet of Things swiftly communicates through data sharing between devices, based upon the use of automation, remote monitoring, via the operation of physical objects and processes. Leveraging the capabilities of IoT, business peoples can achieve useful perceptions, increase efficiency and productivity, and realize a fresh potential for innovation in areas such as healthcare, transport, agriculture, manufacturing, and smart cities. However, IoT also raises concerns about privacy, security and data management that need to be addressed for its widespread and success. The IoT communication technologies are broadly classified into WPAN and LPWAN, those technologies are employed to perform the above-mentioned processes and to overcome challenges.

The Wireless Personal Area Networks (WPANs) comprises of the widely used Bluetooth (BLE) technology having been operating at 2.4 Ghz with coverage range of 300 m, channel bandwidth of 2 Mhz and data rate of up to 1 Mbps for short range communication. BLE is commonly found in personal devices like smartphones, tablets, and wearable technology. Zigbee is a low power WPAN standard designed for home automation, industrial control, and sensor networks, which is being operated at 2.4 Ghz and 900 Mhz with coverage of 10 to 100 m, channel bandwidth of 0.3 to 2 Mhz, and data rate of up to 20–250 kbps. Z-Wave operates at sub-1 Ghz offering better range compared to Zigbee. Similarly, the Low-Power-Wide-Area-Networks (LPWANs) comprises of LoRaWAN which utilizes the LoRa modulation technology operating at unlicensed ISM radio bands, channel bandwidth of 250 khz to 500 khz, data rate of 300 bps to 50kbps.

LoRa WAN enables low power consumption for communication with long range. It's suitable for IoT applications requiring long battery life and connectivity over several kms. Sigfox offers long range and minimal power consumption for communication. It works in frequency bands (unlicensed) with channel bandwidth of 100 Hz, data rate of 100 to 1000 bps and is widely used in applications such as asset tracking, environmental monitoring, smart metering over several kilometres. Next comes the NB-IoT which is called as cellular LPWAN technology standardised according to the third-generation partnership project (3GPP),

NB-IoT works in spectrum bands(licensed) with channel bandwidth of 180 Khz and data rate of few kbps to 10 kbps and provides reliable connectivity for IoT device with low data rate requirements.

In order to cope with the limitations of the aforementioned standards, a newly emerging technology called Wi-Fi HaLow can be recommended. Wi-Fi HaLow is a wireless communication standard developed by the Wi-Fi Alliance specifically for the Internet of Things. Wi-Fi HaLow operates in the sub-1GHz frequency range, penetrating walls and other obstacles more effectively, and was specifically intended for smart home devices, industrial sensors, and other IoT applications where range and battery life are critical. It relies on the IEEE 802.11ah standard and adds some additional functionality. For example, Wi-Fi HaLow improves the power efficiency of devices, allows for thousands of devices per access point, and works with current Wi-Fi technologies.

As IoT continues to expand across multidisciplinary fields, Wi-Fi HaLow offers a predominant solution to address the constrains of IoT deployments and further enabling the system of interconnected smart devices that can communicate smoothly with criteria of conserving energy and extending network coverage. The MAC features comprise of two division namely high scalability (Fast Association and RAW) and low power consumption (TIM segmentation, Target Wake Time TWT and subchannel selective transmission).

For complete network connectivity, devices can link up with a connectivity Point (AP). By enabling the AP to observe every mobile device, association ensure effective frame delivery. But it only happens in wireless infrastructure networks. Only one AP may be associated with a station at once. Association is the process by which sensor nodes are authenticated for the process of adding them to the network, by assigning a unique identifier called Association Identifier (AID). IEEE 802.11ah's access control mechanism during association is Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).

The AP sends out the beacon frame on a regular basis to announce the presence of a wireless network and synchronize all network stations. The channel access in RAW for station is acquired by competing for channel access using the EDCA process flow that is based on their requirements the priority table will be generated according to that the sensor nodes get channel access after backoff period by sensing the channel, whether it is idle or busy. If it senses the channel is busy it waits for backoff period and decrement the counter value till it reaches the zero value which means the channel is free. After the back off period the station starts its transmission in the transmission opportunity phase.

In Distributed Authentication Control (DAC), a beacon interval is broken into smaller intervals known as Authentication Control Slots (ACSs). Stations issue AUTH Requests including a random beacon interval and an ACS. The development of Centralised Authentication Control (CAC) aimed in enhancing the authentication process and positively impacting related mechanisms like association. Within CAC, the AP transmits beacon frames containing an authentication threshold at regular intervals, known as beacon interval (BI). This threshold is introduced to limit the number of nodes participating in the

association process, this is done with utmost care and dynamic adjustment of threshold will lead to minimize collisions and enhance association time.

Frame collisions are known to occur when there are greater number of sensor nodes, and this number rises with frequent retransmissions. To mitigate this, scientists and researchers have devised a unique protocol that speeds up the process by control over the proportion of sensor stations that are allowed to connect. The paper is systematized as follows: Section 2 describes related work in this field. Section 3 analyses the issues with the fast association mechanism and proposes a new adaptive association algorithm. Section 4 is detailed with the results, and we conclude the article in Sect. 5.

2 Literature Survey

The architecture of IoT, the implementation of LoRa technology, and the open issues and challenges in IoT deployment are explained and it emphasizes the need for improved antenna technology, standardized testing, and about the interferences in long-range communication and concludes by advocating for the use of low-profile antennas with LoRa technology for wider scale of IoT implementation [3]. In contrast of providing suggestion to any new association method, rather they provide improvements to the already existing methods in a Wi-Fi Ha-Low system, these are CAC and DAC. Instead of using the primitive definition provided by the standard itself, the integration of a learning step in the association process to dynamically change the window size during the association method to make them less robust in condition with changing contention conditions [4].

The TRC-RBT-GC approach to address resource allocation issues in the Wi-Fi HaLow network for IoT applications involve using Triggered RAW-centric Registered Backoff Time -based channel access along with grouping Control to improve system performance, achieves load balance within Restricted Access Windows slots. The suggested technique is categorized into four phases namely claiming, AP scheduling, scheduled data transmission, and remaining time data transmission. It aims to schedule STAs for channel access based on their RBT values, improving fairness and throughput and discusses the simulation environment, performance evaluation, and the proposed grouping method to achieve better channel utilization. The main advantage is enabling AP to schedule STAs for channel access based on their RBT values without need for backoff count down time [5].

A fast association technique - FASUS is developed based on the existing LILD, they have introduced three new methods that can be used to circumvent the constraints listed in LILD, such as adaptive round numbers, retransmission-upon-failure and authentication threshold holding. [6]. The challenge of managing accesses for a massive number of devices in IoT applications are discussed and proposes a retransmission and RAW optimization scheme, along with a device grouping algorithm, to address these challenges in IEEE 802.11ah networks. Thereby improving the energy efficiency, channel utilization, and access delay by allowing colliding devices to have another transmission chance in the

next slots, changing the amount of RAW slots, and developing a load-aware and distance-based device grouping method. [7].

It also shows fast association mechanism is far better than normal association mechanism explores and reveals the various overheads associated with Association. It also discusses the difficulties in maintaining association and station wake-up and the possible causes of energy inefficiency, delays, and unreliability in all operations [8]. A new algorithm has been introduced for predicting uplink optimal RAW size and will allow many devices to utilize the uplink access efficiently [9]. The comparative analysis of how the Wi-Fi Halow outperforms Zigbee standard with the necessary parameters such as association time, throughput, and delay performance, and network coverage are explained [10].

Some insights into the existing association mechanisms are discussed and also proposes combination of various existing association mechanisms which produce a better solution rather using them alone and highlights the fact of the current RAW model utilized by 802.11ah is flawed in the fact that it requires all node in the group to be of a homogeneous nature, it also show how a heterogeneous set of nodes will perform in each situation using machine learning models [11]. A comprehensive analysis about how the IEEE 802.11ah is suitable for the new era of IoT (NGI) architecture compares existing communication standards, addresses the requirements for NGI and presents an IEEE 802.11ah-based scalable NGI architecture. It also emphasizes the need for energy-efficient protocols, scalability, high throughput, edge computing, low overhead, and adaptive communication technology of NGI and addresses the challenges and the future direction of incorporating IEEE 802.11ah into the NGI architecture. Also includes detailed analysis about the MAC and also PHY layer features of IEEE 802.11ah, performance evaluations, and open research challenges [12].

The author summarizes everything which is known about IEEE 802.11ah so far [13]. A conceptual framework for calculating the number of STAs that is supported by an IEEE 802.11ah to maximum is explained in brief and shows that good Packet Delivery Ratio could be achieved for both uplink and downlink association traffic even if the number of STAs is considerable. [15]. Another focus on the energy consumption aspects of the current RAW implementation in the 802.11ah protocol is discussed in [16]. It shows how the current implementation consumes excess energy; they achieve this using a probabilistic model where the transmission probability of various states of device is taken when sending a packet during single RAW cycle. They find the optimal energy efficiency using simulated annealing.

[17] gives a insights into the introduction of TIM Segmentation which distributes stations in order to manage the process flow and conserve energy. It also reveals that the rate control algorithms is incorporated for adapting the MCS dynamically in Wi-Fi Halow to utilize them for various applications. [18] demonstrates how to build the IEEE 802.11ah PHY, MAC layer protocols in the ns-3 network simulator. Performance exhibited by the DAC solely depends on the parameters defined in the protocol and compares the performance of these algorithms in different scenarios. [19] states that the presence of multiple

Access points might hinder the performance of the algorithm along with other load balancing issues that play in this domain. [20] gives the valid evaluation mechanism utilized in terms of energy efficiency, latency, and throughput which can be used as guidelines for developing dynamic RAW grouping strategies. On the other hand, [21] proposes a sectorized approach to reduce the number of stations within a sector, which allows them for sharing the RAW slots within different groups and overlapped access point thereby mitigating the hidden node problem.

3 Proposed Work

The proposed work exhibits a three-way handshake that way it can handle the collision losses using retransmission. The sensor nodes (STAs) set a timer after transmitting out the request message. If there is a packet loss, the station might have reached time out condition and performs retransmission. Fast association approaches like LILD, FASUS shows that the above retransmissions inject a lot of redundant frames into the network thereby increasing the collision and network set up time. They mitigate the number of redundant frames by incorporating an additional acknowledgement in between Request and Response frames so that, the station node attempts to retransmit request frame only on failure of Acknowledgement instead of retransmission on timeout.

The steps executed by the station nodes as part of FAST association are as follows:

The station receives a beacon from the access point (AP). After receiving the beacon, the station generates a random number R, within the range from 0 to 1024. Then an if statement checks whether R is less than a predefined threshold value for authentication ($AUTH_{th}$). The station waits here for a Distributed Interframe Space period if this condition is true. Alternatively, if it is false, the station waits for next beacon and goes back to the if statement.

When the DIFS period is over, the station senses whether the channel is busy or free. If it found that the channel is busy, it will automatically freeze the count till the channel evolves into free and then goes back to the "Sense Channel" condition. If the channel is free, the station checks if the value of the backoff counter is zero. If it is false, the station waits for one time slot and decrement's the counter value, and then goes back to the "Sense Channel" condition. If it finds that the value as zero that is true, the station proceeds to transmit an authentication request.

After transmitting the authentication request, the station waits for a Short Interframe Space (SIFS) interval and receives an acknowledgment (ACK). Following this, the station receives an authentication response and sends an ACK along with another SIFS interval.

The researchers [6,18] have used this process which involves a four-way handshake between each station node and Access point which is explained in below Fig. 1. Station transmits an authentication request and receives an ACK from AP. Request gets queued up and served by AP whenever it gets access to the medium. AP competes with other nodes to send the response back.

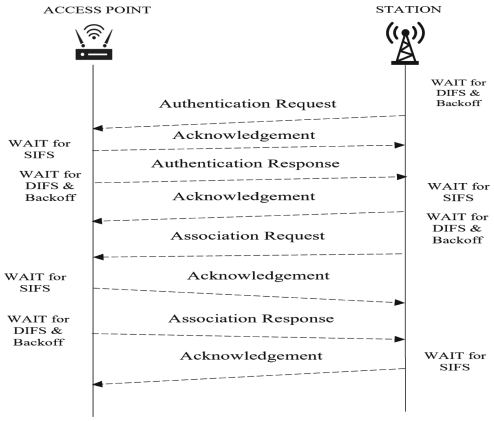

Fig. 1. Four-Way Handshake

The procedure that has been carried out by the AP to serve the authentication / association response is as follows:

This begins by receiving an authentication request and queuing it up for processing. To verify that the authentication request was received, an acknowledgment (ACK) is provided after a Short Interframe Space (SIFS) delay. After that, the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism is utilized to compete for the channel after a Distributed Interframe Space (DIFS) plus a randomized Backoff period. Once the channel is available, an authentication response is transmitted. After a SIFS interval, an ACK is expected to acknowledge the successful transmission.

Another DIFS interval with a Backoff period follows, competing for channel access via CSMA/CA. The process ends upon finding the channel free, sending an association response. It will be followed by a SIFS interval expecting to receive an ACK from the station, indicating that the association response has been successfully delivered. In the same way, association request/response are exchanged between station and AP in an asynchronous manner. But these mechanisms may lead to an increase in average association or link set up time because of additional ACK and additional DIFS time-period introduced while transmitting each Authentication/Association request-response pair.

Sthapit [14] used three-way handshakes during association/ authentication procedure which is shown in Fig. 2. If we consider the time-period required for association/authentication procedure, the minimum total time taken for setting up a link with access point would be greater in four-way handshake when compared with three-way handshake. In IEEE 802.11 ah, a greater number of sensor nodes may try to associate themselves with the AP at the same time during the initial network setup or after power outage which leads to huge collision losses. In this scenario, the timed-out sensor nodes will try to transmit authentication request again that will lead to collision. The time-out period should not

be very small or very large as otherwise it creates unnecessary traffic or reduced performance respectively.

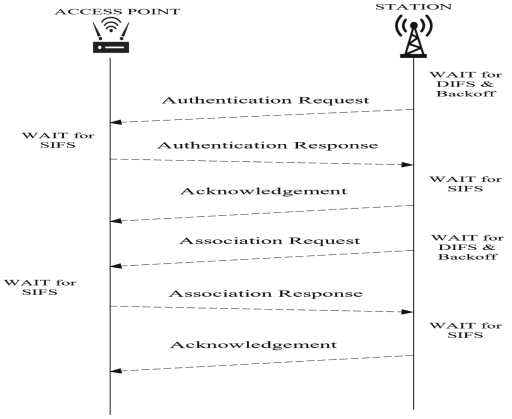

Fig. 2. Three-Way Handshake

In this work, we have considered the above two scenarios and used three-way handshake for the association/authentication process We have set up the time-out period for sensor nodes to be two beacon intervals to reduce collisions. The proposed work is diagrammatically explained in Fig. 3. This algorithm is executed by the AP and station in two modes namely passive and active mode. As our algorithm is focused on large networks, the initial value of the authentication control threshold is set to half of the max value. AP holds the same authentication threshold during the passive mode for the initial two beacon intervals to learn about the network.

Req_R and Req_P represent the number of successful requests served by the AP within the most recent beacon interval and the count of successful requests fulfilled by the AP in the previous beacon interval, respectively. They are used as learning parameters to study the traffic status of this network over time. These variables are initialized with the number of successful requests served by the AP during first beacon interval and second beacon interval respectively. Congestion threshold (CT) approximately represents the $\frac{3}{4}$th of the optimum number of request/response packets that have the potential to be transmitted ideally over the duration of beacon interval. This value is used as the sign of congestion in the network.

Access point enters the active mode from third beacon interval onwards. In this mode, authentication threshold ($AUTH_{th}$) is dynamically calculated at the beginning of each BI and broadcasted to all the sensor nodes through the beacon. This calculation is done based on the values of Req_R, Req_P and CT. If Req_R is greater than CT, then the $AUTH_{th}$ holds the old value without changing it. In this case, decreasing the authentication threshold does not help the nodes as they already started transmitting the requests out.

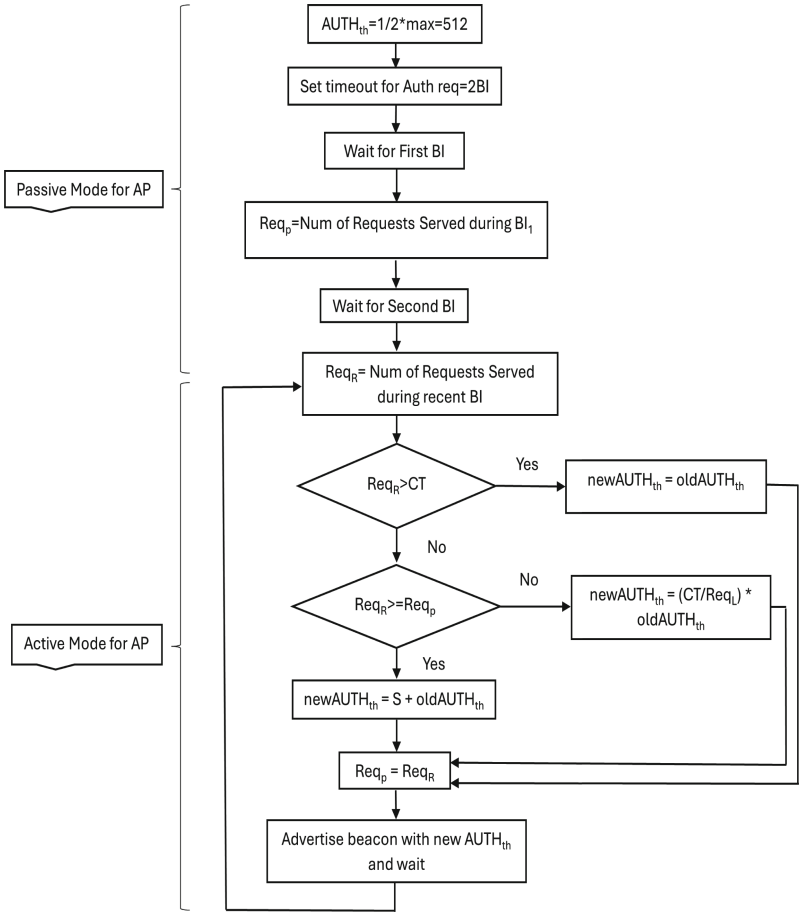

Fig. 3. Adaptive Association Algorithm

When the value of Req_R is more than Req_P, it implies that AP has started receiving more requests and moreover, Req_R is smaller than CT, we linearly increase the value of $AUTH_{th}$. When the value of Req_R is smaller than Req_P, it indicates that $AUTH_{th}$ needs to multiplicatively be increased to accommodate the requests of more nodes. This algorithm adapts to the congestion status of the network and reaches the maximum value finally. The operation of the above proposed algorithm is explained below in the form of pseudocode for easy understanding of the concept.

Algorithm

Passive Mode:

$Initialize \;\; AUTH_{th} = 1/2 * MAX$
$Set \;\; timeout \;\; AUTH_{Req} = 2BI$

$Wait\ \ for\ \ 1\ \ BI$
$Monitor\ \ Req_P = No.\ \ of\ \ requests\ \ served\ \ during\ \ 1BI$
$Wait\ \ for\ \ 2BI$

Active Mode:

$for(Req_R = No.\ \ of\ \ requests\ \ served\ \ during\ \ recent\ \ BI;\ \ Req_R \geq CT;$
$Req_R + +)$
{
$if\ \ Req_R \geq CT$
{
$Update\ \ newAUTH_{th} = oldAUTH_{th}$
}
$else\ \ if\ \ Req_R \geq Req_P$
{
$Update\ \ newAUTH_{th} = S + oldAUTH_{th}$
}
$else$
{
$Update\ \ newAUTH_{th} = (CT/Req_L) * oldAUTH_{th}$
}
$Req_P = Req_R$
$Advertise\ \ beacon\ \ with\ \ newAUTH_{th}$
}

4 Results

We implemented our algorithm using ns3 simulator. Network parameters are listed in Table 1. We considered the network with 7000 nodes. The duration of the beacon interval is set as 102.4 ms. We varied the number of sensor nodes and tested our algorithm. The results are shown in this section. We validated our results against the Linear Increase Linear Decrease (LILD) algorithm.

4.1 Performance Comparison of Association Time in Large-Scale Sensor Networks: ADAPTIVE Vs LLID

The result shown in Fig. 4 depicts a line graph comparing the association time of two different methods, ADAPTIVE and LLID, for varying numbers of sensor nodes within a network.It is clear that from the graph, for both ADAPTIVE and LILD, the association time growth trend is directly proportional to the increase in the number of stations . This increment is logical because when there are more nodes, there is more connection time used due to associations and authentication necessary for traffic to reach the access point. ADAPTIVE had the least association time for a smaller number of stations, but the difference between the two methods was minimal.

To sum up, the ADPATIVE approach sets the benchmarks concerning each form of securing the association times in an overlarge sensor network atmosphere,

Table 1. Network Parameters.

Parameter	Value
Number of nodes	7000
PHY Data rate	650 kbps
Beacon Period	2 ms
Beacon Interval duration	102.4 ms
PHY Header	240 s
MAC Header	14 bytes
Length of Association Request	28 bytes
Length of Association Response	30 bytes
Length of Authentication Request	34 bytes
Length of Authentication Response	34 bytes
Length of ACK	14 bytes
SIFS duration	160 micro sec
DIFS duration	264 micro sec
Slot time	52 micro sec
CW min	16
CW max	1024

particularly when the amount of the nodes increases. In other words, in a real-world situation where thousands of sensor devices need to make the connection to the AP, the use of the adaptive methods would process the network far quicker than LILD. This information can be critical for designing and implementing sensor networks in scenarios where rapid deployment and efficient scaling are necessary.

4.2 Collision Frequency During Network Setup with Increasing Number of Stations: A Comparative Analysis of LILD and ADAPTIVE Algorithms

The graph shown in Fig. 5 represents a comparative analysis between two algorithms, LILD and ADAPTIVE, When the number of stations rises, in terms of the quantity of collisions that happen during network setup. From the graph of the above output data, it is clear that the LILD algorithm has a much higher number of collisions compared to that of the ADAPTIVE algorithm. More precisely, the hits in LILD remarkably increase beyond 5000 stations, which portrait a great decline in scalability and effectiveness. On the other hand, the ADAPTIVE medium collision hits drastically increase at station 5000 as shown in the graph below.

Thus, the results can be taken as a compelling proof of the ADAPTIVE algorithm's superiority in the realm of network setup performance in high-density

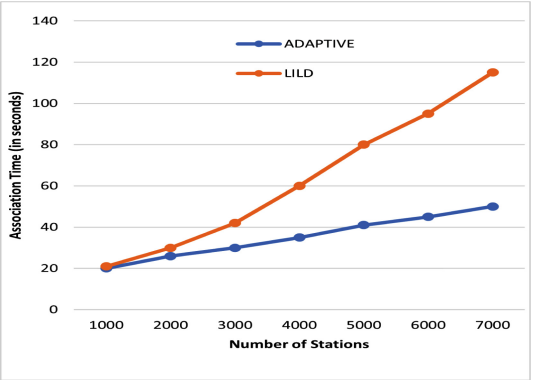

Fig. 4. Aggregate Connectivity Duration across Extensive Node Networks

stations environments. The better collision avoidance frameworks or the algorithm's dynamic nature in adapting to network changes, which enables it to support more nodes with fewer disconnections. Further research into the specifics of each algorithm's approach to handling requests and data packets could provide additional insights into their performance differences. This information would be beneficial for network administrators and engineers who are tasked with optimizing network performance and reliability, especially in contexts with a high volume of devices attempting to connect to a single access point.

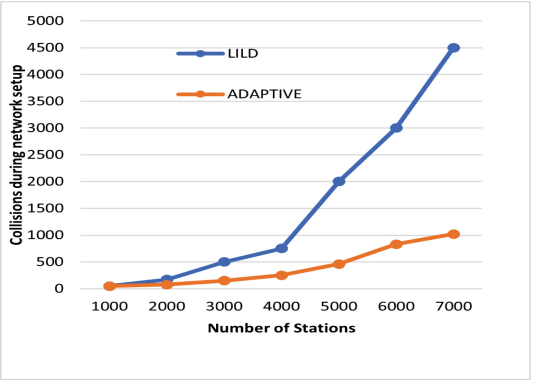

Fig. 5. Collision Count Analysis

4.3 Performance Evaluation of LILD and ADAPTIVE Algorithms in Small-Scale Networks

The results in Fig. 6 above is a line graph shows a comparison of the association time of two different algorithms; LILD and ADAPTIVE. The two algorithms

runs in a small network of sensor nodes that range from 100 to 700 stations count. The performance of the ADAPTIVE algorithm is better than LILD as shown by the much lower rate of association time across the range of stations count. Notably, the graph indicates that the performance of the ADAPTIVE algorithm becomes much better when the number of exceeds 600 sensers. This means that the adaptive calculation of the authentication threshold in the ADAPTIVE approach becomes more effective in a small scale network.

We can attribute this to its responsiveness to the number and the behaviour of the senor nodes in that it reduces the time taken in the association process of each node in the network. Therefore, as many nodes continue to enter the network, the performance is constantly in a check making it hard for one node to majorly affect the network overall performance.

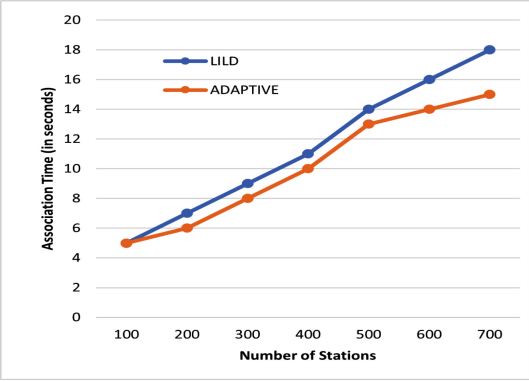

Fig. 6. Connection Duration within Compact Networks

5 Conclusion

An adaptive congestion aware authentication threshold tuning is executed through this work. This method outperforms LILD in terms of association time and number of collisions during network setup. This work can be enhanced by applying machine learning based predictions to study the network status and optimize the measurement of authentication threshold.

References

1. Wang, J., Lim, M.K., Wang, C., Tseng, M.L.: The evolution of the internet of things (IoT) over the past 20 years. Comput. Ind. Eng. **155** (2021). https://doi.org/10.1016/j.cie.2021.107174

2. Kassab, W., Darabkh, K.A.: A-Z survey of internet of things: architectures, protocols, applications, recent advances, future directions and recommendations. J. Netw. Comput. Appl. **163** (2020). https://doi.org/10.1016/j.jnca.2020.102663
3. Sneha, Malik, P., Sharma, R., Ghosh, U., Alnumay, W.S.: Internet of things and long-range antenna's; challenges, solutions and comparison in next generation systems. Microprocess. Microsys. **103** (2023). https://doi.org/10.1016/j.micpro.2023.104934
4. Bankov, D., Khorov, E., Lyakhov, A., Stepanova, E., Tian, L., Famaey, J.: What is the fastestway to connect stations to a Wi-fi Halow network? Sensors (Switzerland) **18** (2018). https://doi.org/10.3390/s18092744
5. Huang, C.M., Hsieh, C.H.: Registered-backoff-time (RBT) based channel access with grouping control for the trigger raw mode of IEEE 802.11ah IoT network. Comput. Netw. **242** (2024). https://doi.org/10.1016/j.comnet.2024.110209
6. Yin, W., Hu, P., Wang, W., Wen, J., Zhou, H.: FASUS: a fast association mechanism for 802.11ah networks. Comput. Netw. **175** (2020). https://doi.org/10.1016/j.comnet.2020.107287
7. Eftekhari, E., Ghahfarokhi, B.S.: Energy and spectrum efficient retransmission scheme with raw optimization for IEEE 802.11ah networks. Ad Hoc Netw. **154** (2024). https://doi.org/10.1016/j.adhoc.2023.103376
8. Ramanna, V.K., Sheth, J., Liu, S., Dezfouli, B.: Towards understanding and enhancing association and long sleep in low-power Wifi IoT systems. IEEE Trans. Green Commun. Netw. **5**, 1833–1845 (2021). https://doi.org/10.1109/TGCN.2021.3085908
9. Park, C.W., Hwang, D., Lee, T.J.: Enhancement of IEEE 802.11ah mac for m2m communications. IEEE Commun. Lett. **18**, 1151–1154 (2014). https://doi.org/10.1109/LCOMM.2014.2323311
10. Ahmed, N., Rahman, H., Hussain, M.I.: A comparison of 802.11ah and 802.15.4 for IoT. ICT Express **2**, 100–102 (2016). https://doi.org/10.1016/j.icte.2016.07.003
11. Tian, L., et al.: Optimization-oriented raw modeling of IEEE 802.11ah heterogeneous networks. IEEE Internet Things J. **6**, 10597–10609 (2019). https://doi.org/10.1109/JIOT.2019.2940251
12. Alam, M., Ahmed, N., Matam, R., Barbhuiya, F.A.: Analyzing the suitability of IEEE 802.11ah for next generation internet of things: a comparative study (2024). https://doi.org/10.1016/j.adhoc.2024.103437
13. Tian, L., Santi, S., Seferagić, A., Lan, J., Famaey, J.: Wi-fi Halow for the internet of things: an up-to-date survey on IEEE 802.11ah research (2021). https://doi.org/10.1016/j.jnca.2021.103036
14. Sthapit, P., Pyun, J.Y.: Station grouping strategy for minimizing association delay in IEEE 802.11ah. IEICE Trans. Commun. **E100B**, 1419–1427 (2017). https://doi.org/10.1587/transcom.2016EBP3306
15. Adame, T., Bel, A., Bellalta, B., Barcelo, J., Gonzalez, J., Oliver, M.: Capacity analysis of IEEE 802.11ah WLANs for M2M Communications. In: Jonsson, M., Vinel, A., Bellalta, B., Marina, N., Dimitrova, D., Fiems, D. (eds.) MACOM 2013. LNCS, vol. 8310, pp. 139–155. Springer, Cham (2013). https://doi.org/10.1007/978-3-319-03871-1_13
16. Wang, Y., Li, Y., Chai, K.K., Chen, Y., Schormans, J.: Energy-aware adaptive restricted access window for IEEE 802.11 ah based smart grid networks. In: 2015 IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 581–586. IEEE (2015)

17. Tian, L., Šljivo, A., Santi, S., Poorter, E.D., Hoebeke, J., Famaey, J.: Extension of the IEEE 802.11ah ns-3 simulation module, pp. 53–60. Association for Computing Machinery (2018). https://doi.org/10.1145/3199902.3199906
18. Tian, L., Deronne, S., Latré, S., Famaey, J.: Implementation and validation of an IEEE 802.11ah module for ns-3, vol. Part F132163, pp. 49–56. Association for Computing Machinery (2016). https://doi.org/10.1145/2915371.2915372
19. Bankov, D., Khorov, E., Lyakhov, A., Stepanova, E.: Fast centralized authentication in Wi-Fi Halow networks. Institute of Electrical and Electronics Engineers Inc. (2017). https://doi.org/10.1109/ICC.2017.7996510
20. Tian, L., Famaey, J., Latre, S.: Evaluation of the IEEE 802.11ah restricted access window mechanism for dense IoT networks. Institute of Electrical and Electronics Engineers Inc. (2016). https://doi.org/10.1109/WoWMoM.2016.7523502
21. Bhandari, S., Sharma, S.K., Wang, X.: Device grouping for fast and efficient channel access in IEEE 802.11 ah based IoT networks. In: 2018 IEEE International Conference on Communications Workshops (ICC Workshops), pp. 1–6. IEEE (2018)