VOL. 18, NO. 1, 2019, 11-15
www.elektrika.utm.my
ISSN 0128-4428

ELEKTRIKA
Journal of Electrical Engineering

Application of Bat Algorithm for The Detection of Hidden Nodes in IEEE802.11ah Networks

Fapohunda Kofoworola O.[1*], Paulson Eberechukwu Numan[1,2], Zubair Suleiman[1], Oladimeji Saliu[1], David Michael[1] and **Kamaludin Mohammed Yusof[2]**

[1]School of Electrical Engineering Technology, Federal University of Technology, Minna, Nigeria.
[2]School of Electrical Engineering, Universiti Teknologi Malaysia, 81310 UTM Skudai, Johor, Malaysia.

[*]Corresponding author: enpaulson2@gmail.com, Tel: +601-680-34922.

Abstract: The occurrence of the hidden node problem in IEEE802.11ah has increases by 41% as compared to previous versions of IEEE802.11 standards. This makes IEEE802.11ah network to be prone to experience high collision and low throughput. Previous efforts to solve this problem has mainly not addressed the issue of locating potential hidden nodes in the network. As a result, the hidden node problem in IEEE802.11ah still remains an open issue. This paper proposes an algorithm that applies bat algorithm for detecting hidden nodes in IEEE802.11ah networks. Our results have shown the effectiveness of this algorithm in detecting hidden nodes. This algorithm can be used to properly manage communication in IEEE802.11ah.

Keywords: Access window, collision, hidden node, IEEE802.11ah, NS-3 and Packet loss.

Article History: received 15 January 2019; accepted 10 April 2019; published 25 April 2019.

1. INTRODUCTION

Technology on wireless fidelity commonly called WiFi has progressed over the years. This has led to the development of WiFi standards which are meant to meet different requirements. Some of which are described in Table 1. Recent development in internet of things has placed a great demand on the increase in the number of interconnection of devices. In order to meet this requirement, the demand on Wireless Local Area Network (WLAN) to connect devices so that they can function automatically also increased. This include the ability to have smart cities, smart houses, healthcare monitoring, industrial automation, agricultural monitoring and smart metering [1]. WiFi then came up with a new task group called "ah". This task group came up with IEEE802.11ah. This was designed to meet up with the requirement of support for large devices, low cost, large coverage area and energy efficient [1] and [2]. There is a general problem that cuts across all these WiFi standards called the hidden node problem. However, this hidden node problem has increased by 41% as compared to previous versions of IEEE802.11 standards. As a result, the IEEE802.11ah network is prone to experience high collision and low throughput [3]. Previous efforts to addressing this issue has mainly not addressed the issue of location potential hidden nodes in the network.

IEEE802.11ah is a sub1GHz network that implements the characteristics of IEEE802.11ac within its frequency range. It has physical (PHY) and Media Access Control (MAC) Layers. The PHY layer operates at a low band width which ranges from 1 to 16MHz allows a transmission range of upto 1km [3]. Modulation and coding scheme (MCS) utilized by IEEE802.11ah includes: binary conventional coding (BCC) which is mandatory and low-density parity check (LDPC) which is optional. The standard is supported by BPSK, QSPK and QAM modulation schemes. Apart from MCS, it also uses Number of Spatial Streams (NSS) and duration of Guard Interval. The MAC layer of IEEE802.11ah introduces channel access mechanisms that attempts to help in addressing the density of the network and energy of the stations. These mechanisms include; hierarchical organization, short MAC header, Traffic indication map (TIM) segmentation, Target Wake Time (TWT), Restricted Access Window (RAW). [4]. The mechanism that deals majorly with hidden node is RAW.

Considering ratio of about 8000 nodes to one access point that exist as a result of their large coverage area, IEEE802.ah adopted a group-based contention as a selection process where a group is allocated to a node in order to minimize packet collision causing network performance degradation that are likely to occur as a result of the hidden node pairs. Restricted Access Window (RAW) which refers to access interval with several time slots where a station competes for time slot during a medium access tried to solve the problem but the hidden node problem was not considered during the allocation of the time slot of RAW [5], this still resulted into station collision as stations that belonged to the same time slot may detect one another. This paper therefore looks into the detection of hidden nodes for easy consideration during the time allocation of RAW slots. Section 2 discusses the related work, 3.0 briefly describes the hidden node problem. Section 4 the proposed method, Section 5 discusses the result while 6 is the concluding part.

Table 1. IEEE802.11 standards

Standards	Characteristics/ Reason for creating it	Date published
IEEE802.11u	It brought about improvement in the area of hotspots and third-party authorization of clients.	2011
IEEE802.11v	It handled the management of the wireless network	2011
IEEE802.11w	It helped to protect management frames	2009
IEEE802.11y	It is 3650-3700MHz operation in the US	2008
IEEE802.11ac	It came up with Very high throughput < 6GHz with improvements over IEEE802.11n in terms of modulation, throughput, wider channels and multiple input and multiple output.	2013
IEEE802.11ad	It introduced a very high throughput of 60GHz	2012
IEEE802.11ae	It came up with the prioritization of management frames	2012
IEEE802.11af	This was done so that TV white space can be used effectively	2014
IEEE802.11ah	It was a smart metering sub 1GHz sensor network	2017
IEEE802.11ai	It was a fast-initial link set up standard	2016
IEEE802.11mc	It handled maintenance of the standard	2015
IEEE802.11md	802.11 accumulated maintenance changes	2020 (predicted)
IEEE802.11aj	It was a China millimeter wave	2018
IEEE802.11aq	Pre-association discovery	2018 (predicted)
IEEE802.11ak	General link	2018
IEEE802.11aq	It handles pre-association discovery	2018 (predicted)

2. RELATED WORK

There has been a general problem called the hidden node problem that cuts across all these standards. This usually occurs when an access point can communicate with node(s) which is not within the communication range of other nodes there by resulting in collision and loss of packets when they send packets at the same time. IEEE 802.11ah suffers from hidden node problem (frequent packet collision) more than networks (IEEE 802.11a/b/n/ac) because of their wide coverage, high number of devices they can support (about 8000 nodes to one access point) and frequent simultaneous sleeping and sending of the nodes (power saving mode) [6], [7] , [8]and [4]. In solving the hidden node problem, most authors like [4] who proposed traffic adaptive RAW optimization algorithm (TAROA) did not consider the detection of hidden nodes. He used the RAW parameters obtained through the estimation of packet transmission intervals of each station to obtain slots that were assigned stations using the frequency were estimated.

After their simulation, it was discovered that through put performance in a dense traffic was improved upon using this TAROA more than when RAW was used although this was not very efficient because of its latency performance. The authors in [5], then proposed a spatial group RAW media access control (MAC) scheme which they based on the location of station. This actually reduce the hidden node problem by reducing collision probability but the hidden node problem could not totally be solved as there are still existing hidden nodes. As a result of this, it still remains an open issue that needs to be addressed. This research therefore will look into how to detect the hidden nodes. Researches in [9] proposed a regrouping algorithm using node transmission time to detect a hidden node. However, two nodes can be out of each other's detection range and this will result in collision if they transmit data at the same time, therefore the is a need for a better hidden node detection method.

3. HIDDEN NODE PROBLEM

The problem caused by a hidden primary user can be compared to the hidden node problem in Carrier Sense Multiple Accessing (CSMA). This is caused by many factors which includes shadowing or multipath fading that is observed by a secondary user observe while sensing frequency bands occupied by primary users. Figure 1 illustrates the hidden node problem.

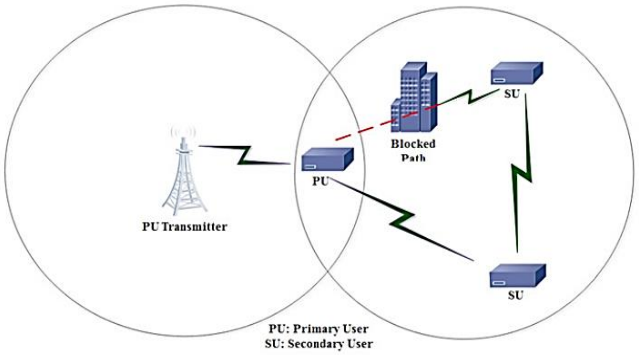

Figure 1. Illustration of the hidden node problem [10]

From Figure 1, the device could not ascertain the state of the primary user due to its position. This will cause an unwanted interference to the primary user. As a result of the hidden node problem, users would require higher detection probability to overcome the receiver's uncertainty. Therefore, this paper proposes an algorithm

that applies bat algorithm for detecting hidden nodes in IEEE802.11ah networks in order to make a decision if the primary user is present or absent.

4. METHOD

Bat algorithm is a biologically inspired algorithm that is based on the echolocation characteristics of micro bats. It has three idealized rules out of which two inspired this detection algorithm, these includes. Bats flying randomly to search for prey. Similarly, for the purpose of this research, STAs are deployed randomly just like the bat. Bats generally use echolocation to sense distance. They have the ability to differentiate between food/prey and background. Similarly, our algorithm will calculate distance between two node pairs asymmetrically. This helps us to determine the hidden nodes. The detection algorithm will be based on bat algorithm where ti is used to represent the data rate at which a station is sending its data, Xi as the position of the node with respect to the AP, fmin as the frequency at which they are operating and the varying wavelength as the perceived signal strength of the AP signal by the station. The formula for received signal strength indicator (RSSI) is the obtained as RSSI (dBm)= -10 logf_0(d)+A where A is the signal strength in dBm and d is the distance. With the algorithm, it can detect the hidden pairs maximally.

The method is as described using the pseudo code below:

Create IEEE802.11ah network scenario with "M" stations STAs. Group M nodes into G groups and associate them with one AP. Define the simulation Parameters [NRaw slot count = SL, Payload size = PL, Beacon Interval = T, Data rate = t, Udp interval = u, Rho = rho]

Let K= (N-1) + (N-2) + (N-3) +…(N-N) // where N is the total number of STAs in a group

Define two solution sets where solution set 1= Not Hidden and solution set 2 = Hidden

Allow multiple nodes within a page or RAW group to send packets to an AP while checking their position or coordinates

WHILE i = 1,2, 3, K// where K is the maximum number of node pair

Calculate the distance D between two node pairs

If D ≤ rho
Choose solution set 1
Else
Choose solution set 2
End if
End WHILE
Report the number of hidden nodes
End.

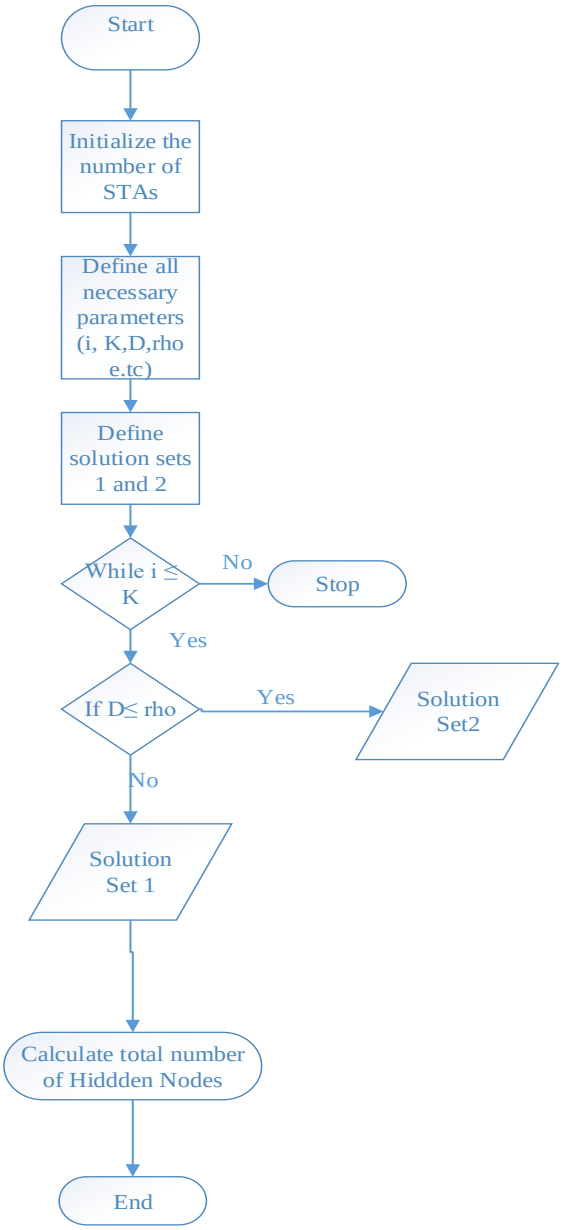

Figure 2. Flowchart of the Algorithm

5. RESULTS

Hidden node problem is a major problem that causes heavy packet drop and degradation of throughput. The authors conducted a research on RAW using these parameters. (packets dropped, hidden node pairs, throughput and packets delivered). It was discovered that as good as the RAW scheme is, it can only be efficient if there is an effective hidden node detection algorithm which is the first step to solving the hidden node problem. As illustrated by figure 1 to figure 4, the graph shows a very great increase in packet drop as the number of STAs increases. This implies that the higher the number of STAs the higher the packet drops and also the higher the hidden nodes which leads to heavy packet drops, hence the effect of the hidden nodes are obvious.

Throughput in Figure 3 decreases from 0.10739 Mbps to 0.0489771 Mbps with increasing number of STAs from 500 to 3000 respectively. This is because, the higher the

number of STAs, the higher the number of packets generated where as the number of slots they compete for remains the same. Hence, there is a great increase in collision rate which results from nodes been hidden from one another.

From Figure 4, the packets delivered first increased with increase in the number of STAs before it started decreasing. Since the same RAW and number of slots were allocated each number of STA, it implies that the packets have more free slots available with lesser number of STAs, there by having a greater number of packets delivered when compared to when a higher number of STAs with a corresponding higher number of packets generated. This also illustrates that the effects of hidden nodes are greater with higher number of STAs.

From Figure 5, the number of packets dropped increases with increase in the number STA because the higher the higher the number of STAs, the higher the number of packets generated to compete for the same time slot. Hence, the higher the collision as more packets tends to compete for the same slot since they are hidden from one another.

Figure 6 shows the corresponding number of hidden node pairs for each STA. This shows that the higher the number of STAs, the higher the number of hidden nodes. This result there by corresponds to the effect seen in Figure 5.

The effectiveness of the algorithm was illustrated from the results obtained using the matrices; throughput, packets delivered, packet drops and hidden nodes detected. The problem of hidden nodes detected can easily be solved by using any other algorithm as this will make provision for easy evaluation of any algorithm designed to solve this problem. This in essence will make us to test any collision reduction algorithm in IEEE802.11ah. this is because this algorithm will assist in calculating and be specific in the number of hidden nodes that a network has at any time such as before and after running any algorithm that is designed to solve this hidden node problem.

6. Conclusion

Hidden node problem (frequent packets collision) which leads to loss of packets affects wireless networks and most especially IEEE802.11ah. To mitigate this problem, it is important to be able to detect these hidden nodes and be able to differentiate it from nodes that are not hidden from one another. This is because hidden node problem is not the only factor responsible for packet loss. If each factor that leads to packet loss is treated individually, then the problem of packet loss can be totally solved. The implementation of this detection algorithm will contribute greatly to solving the hidden node problem and the problem of packet loss at large. This is because it will help in RAW slot allocation and also provides an opening to a new method for solving hidden node problem. Other related topics for future research includes but are not limited to: (1) Provision of appropriate regrouping algorithm based on this detection algorithm, (2) Detection of hidden nodes in a dynamic Network.

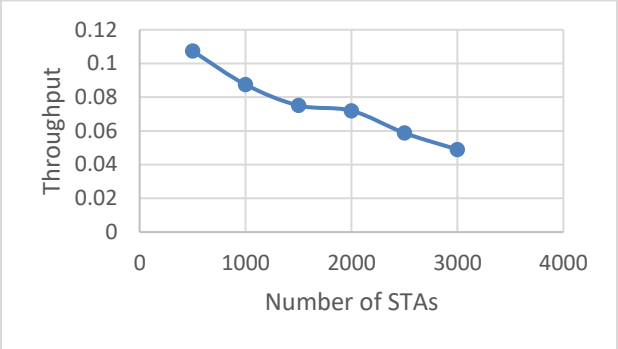

Figure 3: Detection result for throughput

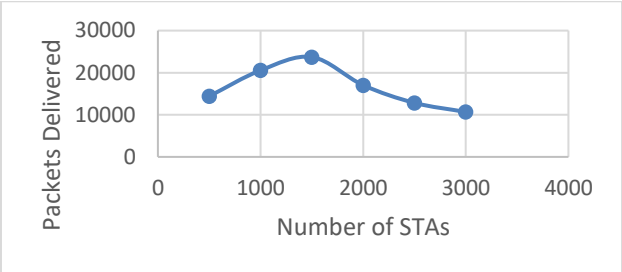

Figure 4: Detection result for packets delivered

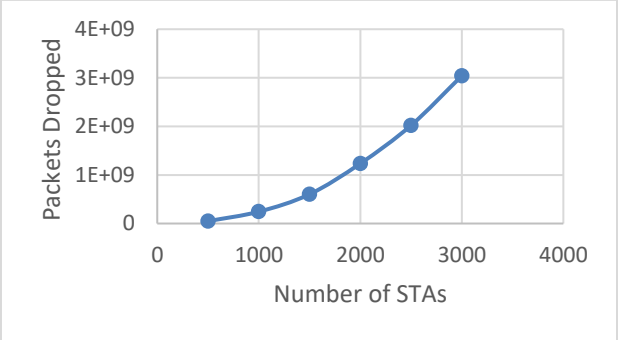

Figure 5: Detection result for packets dropped

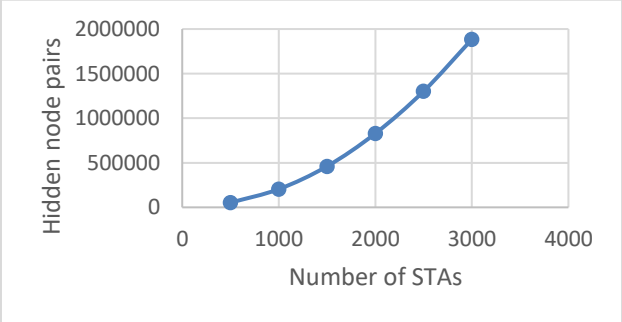

Figure 6: Detection results for hidden nodes pairs

REFERENCES

[1] S. H. Aust, "Advanced Wireless Local Area Networks in the Unlicensed Sub-1GHz ISM-bands," Ipskamp Drukkers, Duitsland, 2014.

[2] W. Sun, M. Choi and S. Choi, "IEEE802. 11ah: A long Range 802.22 WLAN at sub1GHz," Journal of ICT standardization, vol. 1, no. 1, 2013.

[3] L. Tian, J. Famaey and S. Latr´ e, "Evaluation of the IEEE 802.11ah Restricted Access Window Mechanism for dense IoT networks," in Seventeenth International Symposium on a World of Wireless, Mobile and Multimedia Networks, 2016.

[4] M. Dong; Z. Wu; X. Gao and H. Zhao, "An efficient spatial group restricted access window scheme for IEEE 802.11ah networks," in Information Science and Technology (ICIST), 2016 Sixth International Conference on, Dalian, China, 2016.

[5] J. Seo, C. Nam, S. Yoon, and S. Bahk, "Group-based Contention in IEEE 802.11ah Networks," 2013.

[6] Tung-Chung Chang, Chi-Han Lin, Kate Ching-Ju Lin and Wen-Tsuen Chen, "Load-Balanced Sensor Grouping for IEEE 802.11ah Networks," in Global Communication Conference (GLOBECOM), Taiwan, 2015.

[7] P. Sthapit and J. Pyun, "Station Grouping Strategy for Minimizing Association Delay in IEEE 802.11ah," IEICE Transaction communicaton, pp. 1419-1427, 2017.

[8] S. Yoon, J. Seo and S. Bahk, "Regrouping Algorithm to Alleviate the Hidden Node Problem in 802.11ah Networks," May 2016.

[9] J. C. A. LEON, "Evaluation of IEEE 802.11ah Technology for Wireless Sensor Network Applications," Tampere University of Technology, Tampere, Finland, 2015.

[10] P. E. Numan, K. M. Yusof, D. U. Suleiman, J. S. Bassi, S. K. S. Yusof, and J. B. Din, "Hidden Node Scenario: A Case for Cooperative Spectrum Sensing in Cognitive Radio Networks," Indian Journal of Science and Technology, vol. 9, no. 46, 2016.

[11] O. Raesi, J. Pirkanen, A. Hazmi, T. Levanen, and M. Valkama, "Performance Evaluation ofIEEE 802.11ah and its Restricted Acess Window Mechanism," in ICC'14-W7: Workshop on M2M Communication for Next Generation IoT, 2014.