A BAT-INSPIRED ALGORITHM FOR THE DETECTION OF HIDDEN NODES IN IEEE802.11AH NETWORKS

Fapohunda K. O.[1], Zubair S.[2], David M.[3] and Nuhu B. K.[4], Nwaocha V. O.[5]

[1,2,3]Department of Telecommunication Engineering, Federal University of Technology, Minna.
[4]Department of Computer Engineering, Federal University of Technology, Minna.
[5]Department of Computer Science, National Open University of Nigeria.

ABSTRACT

The unique attribute of extended communication range of IEEE802.11ah, has also increased the occurrence of the hidden node problem 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. Previous efforts to addressing this issue has mainly not addressed the issue of location potential hidden nodes in the network. As a result, the hidden node problem in IEEE802.11ah still remains an open issue. This paper proposes a bat-inspired algorithm for detecting hidden nodes in IEEE802.11ah networks. Our preliminary results have shown the effectiveness of the proposed 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, packet loss.*

1. INTRODUCTION

There is a continuous demand for internet of things. Hence, the importance of Wireless Local Area Network (WLAN) to connect devices so that they can function automatically has caused for attention. This has led to the development of different IEEE 802.11 standards that actually have different setbacks. Despite these setbacks, there is still a growing demand for WLANs to enable applications in different domains such as smart cities, smart houses, healthcare monitoring, industrial automation, agricultural monitoring and smart metering (Aust, 2014). In other to get a lasting solution to this, a sub 1 GHz standardization IEEE 802.ah with the advantage of low cost, large coverage area and energy efficient (Aust, 2014) and (Weiping Sun, Munhwan Choi and Sunghyun Choi, 2013) which is on-going emerged among others.

The PHY layer of IEEE802.11ah implements the characteristics of IEEE802.11ac in its sub1GHz frequency. It operates at a low band width which ranges from 1 to 16MHz allows a transmission range of up to 1km (Le Tian, Jeroen Famaey and Steven Latre,

2016) . It utilizes some sets of modulation and coding scheme (MCS) which includes: low density parity check (LDPC) which is optional and binary conventional coding (BCC) which is mandatory. 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 inherited the characteristics of IEEE 802.11ac but 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) Tian et al (2016). The mechanism that deals majorly with hidden node is RAW.

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 (Mengxi Dong ; Zhanji Wu ; Xiang Gao and Huan Zhao, 2016), 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.

The section 1.0 of this paper is the introductory part, 2.0 discusses the related work, 3.0 is the proposed method,4.0 discusses the preliminary result while 5.0 is the concluding part of the paper.

2. REVIEW OF RELATED LITERATURE

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) (Jeong-O Seo, Changwon Nam, Sung-Guk Yoon, and Saewoong Bahk, 2013), (Tung-Chung Chang, Chi-Han Lin, Kate Ching-Ju Lin and Wen-Tsuen Chen, 2015) , (Pranesh Sthapit and Jae-Young Pyun, 2017) and Tian et al (2016). In solving the hidden node problem, most

authors like Tian et al (2016) who proposed traffic adaptive RAW optimization algorithm (TAROA) did not consider the detection of hidden nodes. The authors 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 (Mengxi Dong ; Zhanji Wu ; Xiang Gao and Huan Zhao, 2016), 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 (Sung-Guk Yoon, Jeong-O Seo and Saewoong Bahk, 2016) 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. PROPOSED METHOD

BAT ALGORITHM: Bat algorithm is a biologically inspired algorithm that is based on the echolocation characteristics of micro bats. (Yang, 2010). It has three idealized rules out of which two inspired this detection algorithm, these includes:

1. Bats flying randomly to search for prey with velocity v_i at position x_i. , with fixed frequency f_{min} which can automatically be adjusted. Similarly, for the purpose of this research, STAs are deployed randomly just like the bat.

2. 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 t_i is used to represent the data rate at which a station is sending its data, X_i as the position of the node with respect to the AP, f_{min} 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 $RSSI\,(dBm) = -10\log(d) + A$ 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:

1. Create IEEE802.11ah network scenario with "M" stations (STAs).
2. Group M nodes into G groups and associate them with one AP
3. For a particular group, define objective function $f(x), x = (x_1, x_2 \ldots x_N)$
4. Initialize the number of STAs in the group N and define the other simulation Parameters [frequency range f_{min} to f_{max} , NRaw slot count = SL, Payload size = PL, Beacon Interval = T, Data rate = t, Udp interval = u, Rho = rho]
5. Let K= (N-1) + (N-2) + (N-3) +…(N-N) // where N is the total number of STAs in a group
6. Define two solution sets where solution set 1= Not Hidden and solution set 2 = Hidden
7. Allow multiple nodes within a page or RAW group to send packets to an AP while checking their position or coordinates
8. WHILE i = 1,2,3,...K// where K is the maximum number of node pair
9. Calculate the distance D between two node pairs
10. If D ≤ rho
11. Select solution set 1 as the best solution
12. Else
13. Select solution set 2 as the best solution
14. End if
15. End WHILE
16. Report the number of hidden nodes as processed result
17. End.

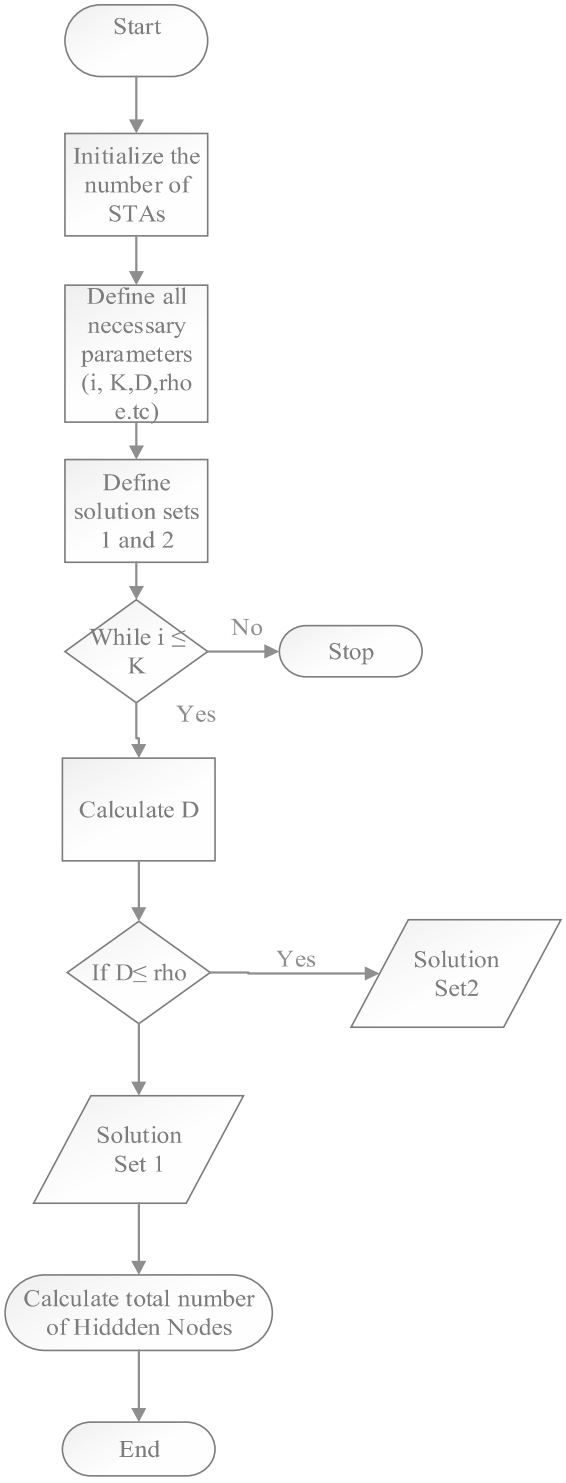

Figure 3.1: Flowchart of the Algorithm

4. PRELIMINARY RESULT

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 and the throughput is very small compared to other parameters, hence the effect of the hidden nodes are obvious.

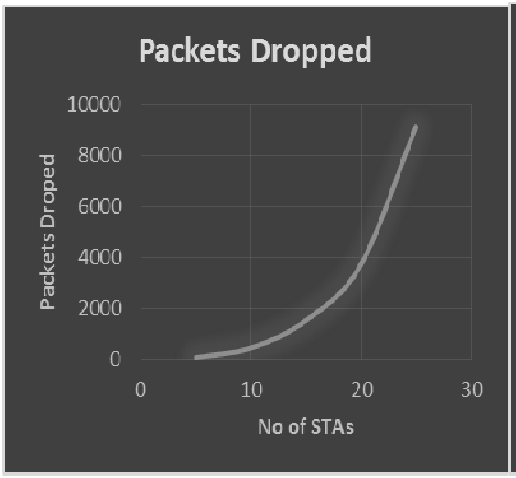

Figure1: Effect of Hidden node problem

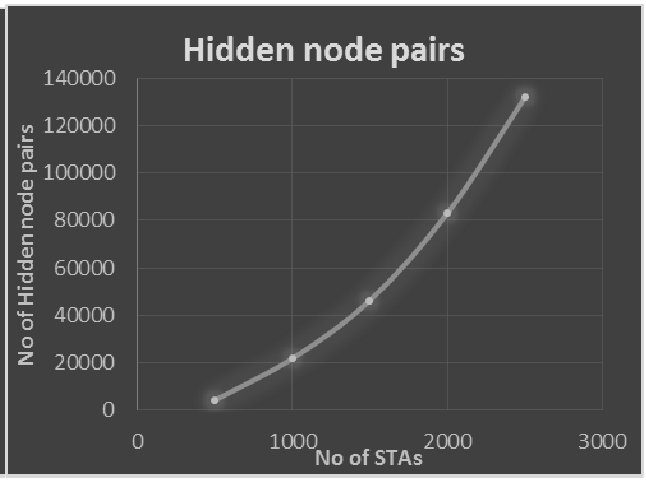

Figure 2: Detected Hidden node pairs

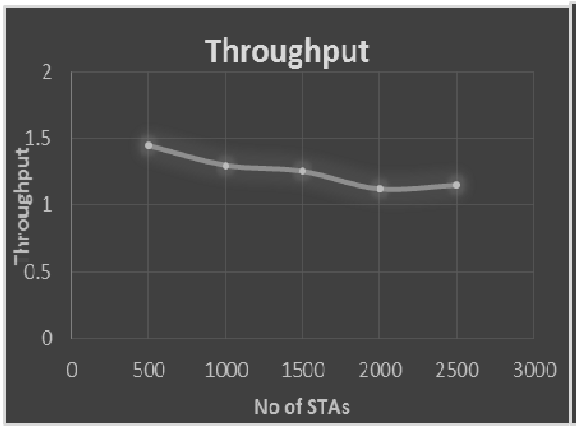

Figure3: Effect of Hidden node on throughput

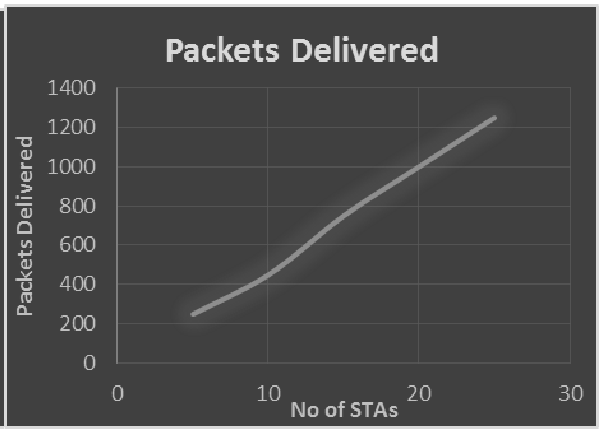

Figure 4: Graph of STAs versus packets delivered

5. PERFORMANCE EVALUATION

The performance of this detection algorithm will be based on the percentage of available hidden nodes before and after using it for RAW slot allocation. As this will help to determine the effectiveness of the algorith6m.

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 develop an efficient hidden node detection algorithm as hidden node problem is not the only factor responsible for packet loss because 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 because it will help in the RAW slot allocation. Other related topics for future research includes but not limited to: (1) Provision of appropriate regrouping algorithm based on this detection algorithm, (2) Detection of hidden nodes in a dynamic Network.

REFERENCES

Aust, S. H. (2014). *Advanced Wireless Local Area Networks in the Unlicensed Sub-1GHz ISM-bands.* Duitsland: Ipskamp Drukkers. Retrieved August 10, 2017

Jeong-O Seo, Changwon Nam, Sung-Guk Yoon, and Saewoong Bahk. (2013). *Group-based Contention in IEEE 802.11ah Networks.*

Le Tian, Jeroren Famaey and Steven Latre. (2016). Evaluation of IEEE 802.11ah restricted Access Window for dense IoT networks. *Seventh International Symposium on world of wireless, Mobile and Multimedia networks*, 1-9.

Le Tian, Jeroen Famaey and Steven Latr´ e. (2016). Evaluation of the IEEE 802.11ah Restricted Access Window Mechanism for dense IoT networks. *Seventeenth International Symposium on a World of Wireless, Mobile and Multimedia Networks* (pp. 1-9). Institutional repository IRUA.

LEON, J. C. (2015). *Evaluation of IEEE 802.11ah Technology for Wireless Sensor Network Applications.* Tampere University of Technology. Tampere, Finland: Tampere University of Technology.

Mengxi Dong ; Zhanji Wu ; Xiang Gao and Huan Zhao. (2016). An efficient spatial group restricted access window scheme for IEEE 802.11ah networks. *Information*

Science and Technology (ICIST), 2016 Sixth International Conference on. Dalian, China: IEEE.

Orod Raesi, Juho Pirkanen, Ali Hazmi, Toni Levanen, and Mikko Valkama. (2014). Performance Evaluation ofIEEE 802.11ah and its Restricted Acess Window Mechanism. *ICC'14-W7: Workshop on M2M Communication for Next Generation IoT* (pp. 460-466). IEEE.

Pranesh Sthapit and Jae-Young Pyun. (2017). Station Grouping Strategy for Minimizing Association Delay in IEEE 802.11ah. *IEICE Transaction communicaton*, 1419-1427.

Sung-Guk Yoon, Jeong-O Seo and Saewoong Bahk. (2016, May). Regrouping Algorithm to Alleviate the Hidden Node Problem in 802.11ah Networks.

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

Weiping Sun, Munhwan Choi and Sunghyun Choi. (2013). IEEE802. 11ah: A long Range 802.22 WLAN at sub1GHz. *Journal of ICT standardization, 1*(1).