Detecting MAC Misbehavior of IEEE 802.11 Devices within Ultra Dense Wi-Fi Networks

Conference Paper · June 2018

DOI: 10.1109/ICT.2018.8464931

3 authors, including:

Shahwaiz Afaqui
Universitat Oberta de Catalunya
22 PUBLICATIONS **209** CITATIONS

SEE PROFILE

Ronan Farrell
National University of Ireland, Maynooth
188 PUBLICATIONS **603** CITATIONS

SEE PROFILE

Detecting MAC Misbehavior of IEEE 802.11 Devices within Ultra Dense Wi-Fi Networks

M. Shahwaiz Afaqui
Wireless Networks Research Lab,
Universitat Oberta de Catalunya, Spain
Email: mafaqui@uoc.edu

Stephen Brown
Department of Computer Science
Maynooth University, Ireland
Email: Stephen.Brown@mu.ie

Ronan Farrell
Department of Electronic Engineering
Maynooth University, Ireland
Email: Ronan.Farrell@mu.ie

***Abstract*—The widespread deployment of IEEE 802.11 has made it an attractive target for potential attackers. The latest IEEE 802.11 standard has introduced encryption and authentication protocols that primarily address the issues of confidentiality and access control. However, improving network availability in the presence of misbehaving stations has not been addressed in the standard. Existing research addresses the problem of detecting misbehavior in scenarios without overlapping cells. However, in real scenarios cells overlap, resulting in a challenging environment for detecting misbehavior. The contribution of this paper is the presentation and evaluation of a new method for detecting misbehavior in this environment. This method is based on an objective function that uses a broad range of symptoms. Simulation results indicate that this new approach is very sensitive to misbehaving stations in ultra dense networks.**

I. Introduction

IEEE 802.11 based Wi-Fi networks have become an integral part of today's indoor communication due to its ease of deployment and cost efficiency. Its popularity and wider acceptance has resulted in dense deployments in diverse environments to cater for the huge traffic demands of end nodes.

The IEEE 802.11 protocols were designed with the assumption that all stations that want to communicate would follow specific predefined rules to transmit and receive data. IEEE 802.11 in its current form includes security protocols such as WEP, WPA, IEEE 802.11i and IEEE 802.11w that use cryptographic checks for data and management frames [1]. However, these protocols only deal with vulnerabilities related to unauthorized access and confidentiality breaches. As a consequence, the IEEE 802.11 standard has been criticized for not including comprehensive security solutions to protect all the entities within the network.

The basic medium access mechanism defined in the IEEE 802.11 standard [2] is the Distributed Coordination Function (DCF). This mechanism is executed locally at each station and is used for contention resolution. It employs the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism for contention coordination (i.e. minimizes collisions) and random backoff to avoid collision (i.e. provides equal fairness guarantees to each communicating stations).

Due to the characteristics of CSMA/CA, the Medium Access Control (MAC) of IEEE 802.11 is very sensitive to malicious attacks. A cheating station not complying with the defined rules of engagement can improve its throughput and latency at the expense of other stations by reducing the overall throughput and fairness of the network [3]. Particularly for the dense deployments encompassing numerous Overlapping Basic Service Sets (OBSS) with asynchronous interference (which is a critical factor in frame error rate performance), a cheating station can have a cascading effect on neighboring overlapping cells. While the malicious station can benefit from a modified MAC, its excessive channel access can lower the performance on stations present in the neighboring cells. In order to tackle selfish behavior in dense deployments, it is important to first employ a mechanism that helps in the detection of malicious entities and then take the appropriate countermeasures. This detection procedure can be instrumental in countering the cascading performance degradation effect that an adversary can induce in ultra dense networks.

A. Related work

Even through there is much research work on the detection of greedy stations within a CSMA/CA based network, to the best of our knowledge this is the first work that aims to perform detection in ultra dense IEEE 802.11 networks. Even though OBSS results in good coverage, the overlapping of numerous Access Points (AP) and the use of common channel results in an amplification of problems faced in traditional non-dense networks [4].

An IEEE 802.11 station in infrastructure mode can attain selfish behaviour by varying either the MAC layer or the physical layer parameters. At the physical layer, increases in the Carrier Sense Threshold (a parameter which indicates the occupancy of the channel) and the transmit power could benefit a station. In this paper, we address the MAC layer manipulations.

A selfish station can manipulate the MAC layer parameters, such as Contention Window (CW) size, Inter Frame Space (IFS) [5] and the remaining transmission duration, responsible for channel access which enable it to wait for a shorter time for transmission than the legacy devices that behave according to the defined rules (i.e. the device increases its chance of winning the contention based channel access). While manipulations in IFS are relatively easy to detect due to the constant behavioral variations, the non-deterministic nature of the IEEE 802.11 MAC does not provide the receiver any information on the transmitter's backoff values and there is no method to detect whether the station selfishly selected a shorter backoff time.

Various techniques have been proposed for the detection of MAC misbehaving stations in IEEE 802.11 based Wi-Fi networks. A common method to detect selfish behavior relies on monitoring the overall network statistical information and checking whether the expected results match the observed results. The mode of detection in [6] and [7] is based on

 DOI: 10.1109/ICT.2018.8464931

extensive monitoring and analysis of shared frames by the AP with the help of additional modules. A lightweight fair-share detector is designed in [8] which exploits the fairness property of the complete network. By identifying the number of successful transmissions, the AP calculates the throughput of each node and identifies a cheater based on highest throughput. However, the authors have evaluated their proposed scheme for a simple one cell scenario. Also, for the case of OBSS, other parameters (such as Frame Error Rate and latency) could assist in the anomaly detection. In [9] a new method is presented to detect the malicious entity for IEEE 802.11 network using a novel metric called Beacon Access Time (BAT). This scheme was based on the principle that transmissions of beacons have priority over any other transmission and, thus, can be used to monitor the activity within WLAN network area from its AP (i.e. not requiring any modification to legacy client stations). In spite of the simplicity of BAT based scheme, the effectiveness of this scheme was more evident when less than 10 stations were communicating to an AP.

None of the above mentioned works and others in literature address the problems of detecting misbehaviour in OBSS environments.

B. Contributions

To address the OBSS scenario and the limitations of existing cheater detection mechanisms, in this paper we propose a passive detection scheme that can be implemented on each AP. Particularly for the cascading performance degradation in OBSS scenario, APs must collaborate with neighboring APs to evaluate the change of performance. Therefore, the proposed scheme is made to operate at the network level as well as the cell-local level. The proposed method detects misbehaving nodes on the basis of passive observations at runtime without incurring any extra overhead or modifications required in the IEEE 802.11 MAC. The main contributions of this paper are:

- We address the problem of detecting selfish nodes in ultra dense Wi-Fi environments, and propose a simple, yet accurate, detecting algorithm. We define an objective function that is used in the detection process.
- The proposed solution is based on the fact that existence of a selfish node causes global as well as local variations (in overlapping cells). If significant variation with respect to the default/reference objective function is detected, the cheating selfish device can be isolated and detected.
- In depth analysis and simulations results are provided corresponding to an ultra dense environment where different links experience variations in interference (frame error). Results are also compared with other metric used in literature, such as PDR [10] for the non-OBSS case.

To the best of our knowledge, our proposal is the first AP-based MAC misbehavior detecting solution for the challenging ultra dense Wi-Fi environment. The same set of problems are also expected to occur in other future ultra dense networks (such as LoRa, Sigfox, IEEE 802.11ah, etc.).

The remainder of the paper is organized as follows. Section II describes the basic features of IEEE 802.11 MAC and the operations of a selfish station. Section III describes the metrics used in the detection process. Section IV provides details of the simulation environment. Section V, describes the performance evaluation results along with an in-depth analysis. Finally, conclusions and future work directions are presented.

II. Preliminaries

In this section, we briefly describe the basic features of IEEE 802.11 MAC and methods used by misbehaving selfish stations to gain unfair advantage. According to IEEE 802.11e amendment, the Access Point (AP) broadcasts the default values of the MAC parameters. A selfish node can manipulate these parameters to increase its channel access opportunities and unfairly gain more resource.

A. IEEE 802.11 MAC

The Enhanced Distributed Channel Access (EDCA) channel access mechanism of IEEE 802.11e standard extends the former Distributed Channel Access (DCA) mechanism through the generalization of the MAC parameters. These parameters control the behavior and randomness of stations when accessing the channel.

DCF is a distributed access mechanism which is implemented independently at each station and utilizes a binary exponential backoff to react to collisions and physical carrier sensing to prevents simultaneous transmissions. The physical layer carrier sensing method, called Physical Clear Channel Assessment (PHYCCA), is used to observe the channel conditions before transmission (e.g. if the energy level detected on the shared channel is greater than a predefined threshold, it means that the channel is occupied and, thus, the transmitter should abstain from transmission).

The DCF mechanism imposes an idle interval between two consecutive frames, called Interframe Space (IFS). While accessing the channel, one of the two situations can occur:

- If the channel is sensed idle by the intended transmitter for a period of time greater or equal to a Distributed Inter Frame Space (DIFS), it initiates transmission.
- If the channel is sensed busy during or after DIFS, the station waits for a random backoff interval again before sensing the channel.

Each station generates a random backoff time within a CW size before attempting to transmit again. A slotted binary exponential backoff interval is chosen in the range [0, CW-1]. The CW starts with a minimum value of CW_{min}. After each unsuccessful transmission, the CW value is doubled upto the maximum CW_{max}. The relation between CW_{min} and CW_{max} is given by:

$$CW_{max} = 2^m \times CW_{min} \tag{1}$$

where, m is the maximum increasing factor and takes a value between 0 and 5.

If a station intending to transmit, detects the channel busy, the backoff timer is frozen and resumed only when the channel is detected idle for more than DIFS period. The backoff timer is decreased while the channel is sensed idle. The random backoff procedure is also followed between transmission of two consecutive new transmissions from the same transmitter, even if the channel is sensed idle.

Two techniques are used for frame transmission in DCF: the basic two-way handshake (see Figure 1) and the optional

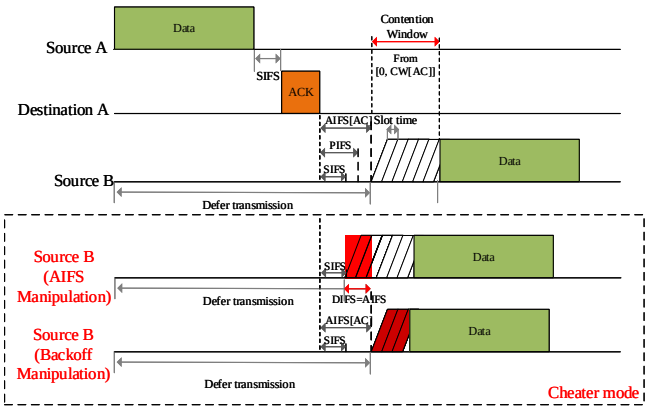


Fig. 1: Frame transmission of basic handshake in IEEE 802.11 MAC with a misbehaving station.

TABLE I: Default DCF and EDCA parameters.

Parameters		CWmin	CWmax	AIFSN	TXOP limit
DCF		aCWmin	aCWmax	2	
EDCA	AC_BK	aCWmin	aCWmax	7	0
	AC_BE	aCWmin	aCWmax	3	0
	AC_VI	(aCWmin+1)2-1	aCWmin	2	3.008 ms
	AC_VO	(aCWmin+1)4-1	(aCWmin+1)2-1	2	1.504 ms

four-way handshake[1]. In two-way hand shake, an ACKnowledgment (ACK) frame is transmitted by the successful reception of packet by the receiver after a period of time called the Short Interframe Space (SIFS). It is a short interval used to split transmissions belonging to a single dialogue (DATA-ACK). A transmission with ACK not received is deemed a collision by the transmitter. SIFS is assigned a value that is shorter than DIFS so as to restrict stations to detect the channel to be idle until the end of the ACK. For non-QoS DCF operations, DIFS is related to the SIFS by the following relation,

$$DIFS = AIFS = AIFSN_{DCF} \times \sigma + SIFS \qquad (2)$$

where, Arbitration Interframe Space (AIFS) is an EDCA parameter which is similar to DIFS in DCF mechanism, Arbitration Interframe Space Number (AIFSN) is used by a station in order to determine the specific AIFS (Arbitration Interframe Space) value for each of the four EDCA (Enhanced Distributed Channel Access) classes. The AIFSN value is transmitted by the AP to stations and its value must be greater than or equal to 2 for all non-AP stations. σ corresponds to the slot time.

EDCA mechanism builds on DCF scheme by providing differentiated transmission services for the support of Quality of Service (QoS). Each frame arriving at the MAC with defined priority is mapped into four Access Categories (AC). These categories are, from the highest priority: Voice (AC_VO), Video (AC_VI), Best effort (AC_BE), and Background (AC_BK). As highlighted in Table I, each category has its own set of medium access parameters, which are responsible for traffic differentiation. Also, Transmission Opportunity (TXOP) in EDCA defines a period of time for which a station accessing the channel is allowed to transmit multiple frames without using channel access procedure for all the frames.

The advantage of EDCA is that it guarantees the same probability of channel access for all the stations intending to transmit over the shared channel.

[1]In this paper, we explore the MAC misbehaviour when the default two-way handshake mechanism is used.

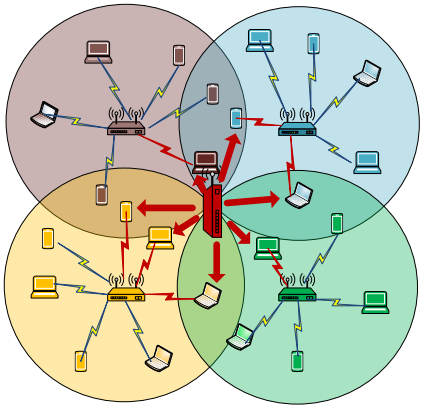


Fig. 2: Impact of malicious device in dense deployments.

B. MAC misbehaviour models

As highlighted above, the DCF scheme does not provide a centralized channel access mechanism and requires a co-operative mode of operation by all the participating stations. Hence, it is very vulnerable to malicious entities operating over the shared medium. Particularly, for the case of dense deployments, there is a need to find solutions that enable detection of adversaries, so as that the performance of multiple overlapping cells is not compromised. A selfish malicious station, over the cost of other stations, can manipulate its MAC parameters to improve channel access opportunities that can result in unfair gain in shared resources (such as throughput, latency and so on).

As indicated by Figure 2, a cheater can increase its transmission rate and cause collisions at stations concurrently receiving from other sources. This problem is further complicated by the presence of numerous hidden stations in densely co-located Wi-Fi cells, where transmitters might be unable to hear transmissions by stations in neighboring BSS and continue to retransmit frames up-till retry limit of the backoff procedure. Thus, adding to the problem, these retransmissions result in cascading effect, where a cheating device can cause a wide spread impact in high density IEEE 802.11 deployments from a single location. A greedy station can manipulate the aforementioned DCF protocol parameters to increase the probability of channel access:

- Using a smaller SIFS value in the optional four-way handshaking mechanism could affect surrounding neighbors to wait for longer periods by setting their NAV to a longer value.
- When the channel is idle, the station can transmit in a duration less than DIFS and upto SIFS.
- The station can reduce the back-off time by selecting a small fixed contention window. This could be achieved by lowering either the minimum contention window or the maximum contention window size.
- For the AC, a station using voice/video can retain the access of the shared medium by violating the TXOP limit parameter and thus sending excessive frames upon a single transmission.

In this paper, we address the DIFS and contention window

manipulations by the cheaters.

III. System model and assumptions

In this section, we first introduce the OBSS network environment and terminologies used in presenting the proposed scheme. Then we explain the basics of the misbehaviour detection framework that compares network statistics with respect to normal expected behaviour.

A. Ultra dense Wi-Fi network

We define an ultra dense network as a network in which every cell overlaps with at-least one other cell. That is an AP can hear beacon frames from at least one other AP. Ultra dense networks are required to provide adequate bandwidth to numerous Wi-Fi stations.

B. Network setting

In our analysis, we consider the scenario defined by the Task Group 802.11ax (TGax) in [11], which consists of a multi-floor residential building (see Figure 3). It includes 100 apartments and had the following specifications:

- 5 floors
- 2×10 apartments in each floor
- Apartment size: 10m×10m×3m
- Building type: Residential
- External wall type: Concrete with windows

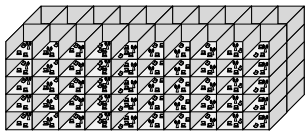


Fig. 3: Layout of ultra dense Wi-Fi deployment in residential building.

A single AP was randomly placed within the walls of each apartment. M (where $M = 10$) non-AP stations were placed around each AP randomly. Varying number of BSS were deployed and all cells used the same frequency channel. We focus our study on the use of 2.4 GHz band because it is more restricted in dense environments (due to only 3 non-overlapping channels).

C. Evaluation metrics

Our scheme uses the following metrics.

1) Aggregate Throughput: is the sum of all successfully received data frame at the destinations.

2) Fairness: Jain's fairness index is the standard traditional measure of network fairness. It is calculated by the following expression [12]:

$$F_J = \frac{(\sum_{i=1}^{n} \beta_i)^2}{n \sum_{i=1}^{n} \beta_i^2} \tag{3}$$

where, β_i is the normalized throughput (in kbps) of the i-th flow and n is the number of competing connections. Absolute fairness is attained when $F_J = 1$ (i.e. all stations get the same data rate) and absolute unfairness is achieved when $F_J = 1/n$. Jain's fairness index is maximized when differences of throughput among different flows minimizes.

3) Frame Error rate (FER): is calculated by:

$$FER = 1 - FSR \tag{4}$$

where FSR is the frame-success-ratio and is calculated by counting the number of received Acknowledge[2] (ACK) frames and the transmitted data frames during a time window.

4) End-to-end-delay: is the average of all mean delays for all non-AP stations. The mean delay includes the transmission, queuing and contention delays for IEEE 802.11 frames. This parameter that can only be counted at the non-AP station and could be communicated to the AP using IEEE 802.11k Radio Resource Management (RRM) frames.

5) Packet Delivery Ratio (PDR): is the ratio of actual packet delivered to total packets sent. This parameter can be predicted by an AP.

Evaluation of these metrics in a distributed network requires additional feedback to the AP. We envisage that IEEE 802.11k amendment is a good candidate for supporting this.

D. Objective function

The goal of any cheating device in IEEE 802.11 network is to gain unfair access and increase its performance at the cost of other stations. Identifying malicious behaviour by evaluating multiple metrics is more effective than using a single metric as shown in Section V. These multiple metrics are incorporated into a single value using an objective function based on our previous work [13][3]. In an ultra dense network, the symptoms of malicious behaviour can be seen both locally (within a cell and its immediate neighbours) and globally throughout the entire network. As shown in Figure 4, the same objective function is used at both levels. Formally, this objective function for the network, called Network Objective Fuction (NOF) can be represented as follows:

$$NOF = \frac{Throughput_{Agg} \times F_J}{Delay_{Avg} \times FER_{Avg}} \tag{5}$$

where, $Throughput_{Agg}$ is the aggregated network wide throughput[4], F_J is the fairness in the network, $Delay_{Avg}$ is the average end-to-end delay and FER_{Avg} is the average FER of all the links.

Individually, each AP also calculates its own objective function by using cell statistics. The Local Objective Function (LOF) is calculated by obtaining the average objective function of neighboring overlapping cells (i.e. a cell that hears beacons of OBSS generates the LOF) and the cell that includes a cheating station.

All the APs in the network that employ the cheater detection schemes use this objective function to learn and adapt so as to find the variations required for cheater detection.

[2] In IEEE 802.11, all successfully received frames are explicitly acknowledged.

[3] The same objective function was used to evaluate the effectiveness of novel AP-managed uplink transmit power control methods proposed to improve the spatial reuse.

[4] Aggregate throughput only does not account for how resources are shared among different clients.

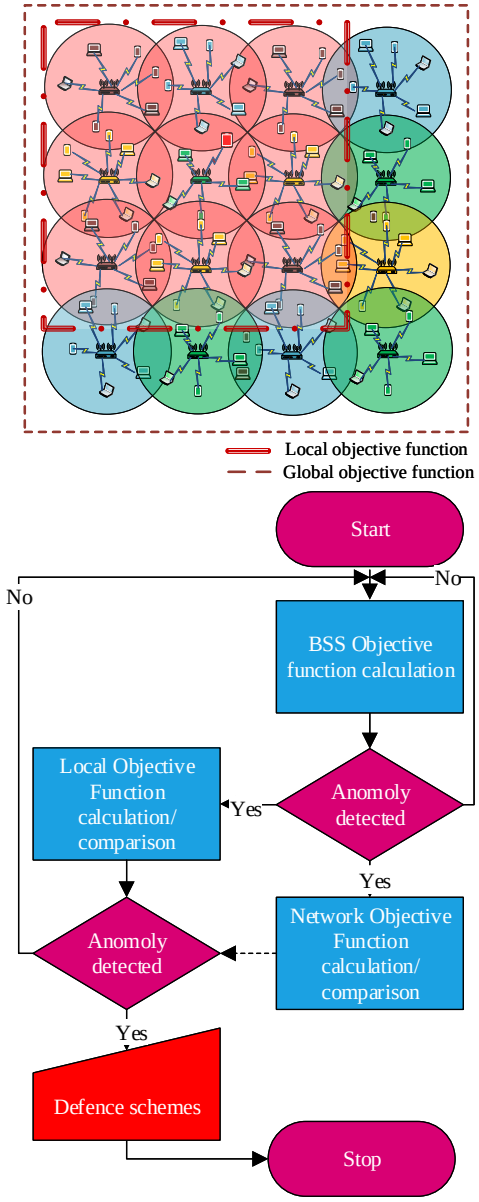


Fig. 4: Objective function calculations in the network.

E. Inter-AP communication

Even through the legacy IEEE 802.11 standard does not specify the means by which two APs could communicate with each other, there do exist propriety solutions by different vendors. Also, in dense managed deployments, AP's are generally connected through a Distributed System (DS) which is a wired network that enables inter-AP communication.

Also, an AP can independently estimate its own objective function and announce that value in its beacon frames, e.g. using beacon stuffing as suggested in [14].

IV. Simulation Setup

The simulations were carried out using the NS-3 network simulator with the Hybrid Building propagation loss model [15]. NS-3 has been found by TGax to provide consistent results [16] and provides the ability to trace cases of problems. Enough simulations were run to achieve 95% confidence intervals (a minimum of 12 runs for each case and the simulation time was 35 seconds). The data rate used for each non-AP station is 3 Mbps guaranteeing saturation in the scenarios addressed. We considered uplink transmission[5], where each non-AP station was in saturation condition[6] (i.e. stations always have frames to transmit).

TABLE II: Physical and MAC layer parameters for simulation.

Parameter	Values	Parameter	Values
Wireless Standard	IEEE802.11n	Packet size	1000 bytes
No. of BSS	32	No. of client per AP	10
Frequency band	2.4 GHz	Transmission power of STA and AP	16 dBm
Physical transmission rate	MCS 7 for data frames, MCS 0 for Control/management frames	Antenna gain	1 dB
Propagation loss model	Hybrid buildings propagation loss	Noise figure	7dB
Wall penetration loss	12dB	Fading model	not used
Floor penetration loss	17dB	Auto Rate Fallback (ARF)	not used
Guard interval	Short	Data preamble	Short
Channel width	20MHz	Beacon Interval	100ms
Aggregation	not used	RTS/CTS	disabled

TABLE III: MAC layer parameters.

Parameter	Cheating Stations	Legacy Stations
CW_{min}	2, 4, 6, 8, 10, 12, 14	16
CWmax	64, 128, 256, 512	1024
DIFS(μs)	10, 19	28
Slot time (σ)(μs)	9	9
AIFSN	0, 1	2

The description of Physical and MAC layer parameters used within our simulation are detailed in Table II. The MAC layer parameters used by cheating devices in the ultra dense Wi-Fi deployment are highlighted in Table III. For traffic generation, we use Constant Bit Rate (CBR) UDP sources in order to evaluate raw capacity at the MAC layer, without the interference of the variations that produce the elastic behavior of the different versions of TCP. CBR is one of the real-time traffic category used by applications that request fixed amount of bandwidth. CBR traffic offers a constant load.

V. Performance Evaluation and Discussion

In this section, we assess the effectiveness of our proposed mechanism for cheater detection in ultra dense Wi-Fi network. Each AP runs our detection algorithm. We compare the performance of objective function and PDR calculation in the presence of a cheating device with the case when no cheater is operational. As highlighted below, the significance of the proposed scheme is its operation at multiple levels of the network.

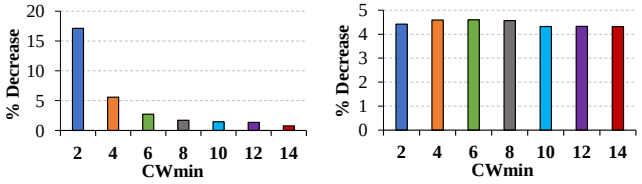
A. Cheaters with CWmin manipulations

Following a DIFS period, stations willing to transmit a frame will back off for a random number of time slots chosen between 0 and the value of the contention window CW. The default value of minimum CW, CWmin is 16. A cheater can utilize lesser CWmin value than 16 which can reduce its backoff and thus increase its access probability.

1) Single cheater in the network: For the cheater CW_{min} value of 2, there is a more than 40% decrease in the objective function of the BSS. In-order to avoid false reporting, in the

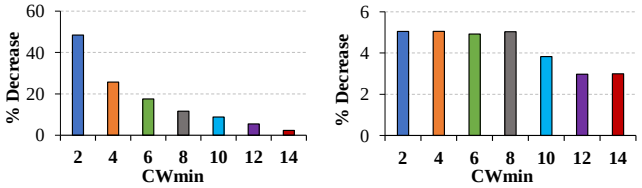
[5]We evaluate the performance over uplink transmissions because it is the worst case in terms of contention.

[6]Saturation is used to explore maximum capacity.



(a) LOF. (b) Local average PDR.

Fig. 5: One cheater in the network reducing CW_{min}.



(a) NOF. (b) Average network PDR.

Fig. 6: One cheater per cell in the network reducing CW_{min}.

next phase, the BSS collects the LOF. Figure 5a indicates that the OBSS are greatly impacted and Figure 11a shows that the malicious device gains considerably. PDR results in Figure 5b show a consistent rise. However, the NOF for all CW_{min} values do not show a decrease (e.g. for CW_{min} value of 2, it decreases by 1.2% only). Thus, at the local level, the OBSS can collaborate to detect a cheating station.

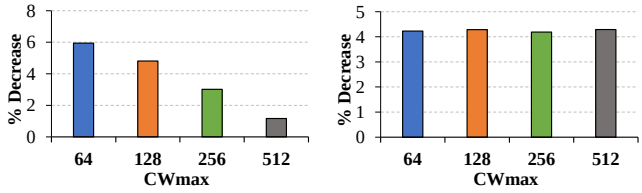
2) One cheater per cell: Next, we evaluate the case where 10% of the non-AP stations behave as cheaters by progressively reducing the CW_{min} value. All APs in the network collaborate together to calculate the NOF. Figure 6a show near 50% decrease in network wide performance. Even though Figure 6b shows the reduction in PDR, it is not as sensitive as the NOF. As highlighted in Figure 11b, the cheating devices do not gain extensive benefits. However, the detection mechanism is able to detect multiple cheating stations.

B. Cheaters with CWmax manipulations

As mentioned in section II, AP and the well behaving non-AP stations change the backoff after a frame loss. If the selfish station used a small CW_{max}, its CW does not become large and the CW is not increased even upon failure of a transmission. However, as the values of CW_{max} used for evaluation are greater than the CW_{min}, the collision probability will be less and the cheaters will gain less from CW_{max} misconfiguration.

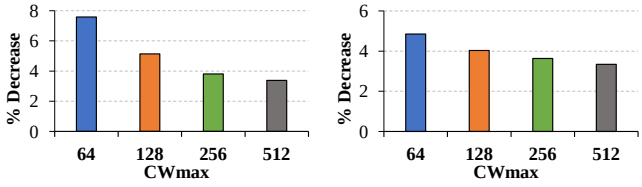
1) Single cheater in the network: Even though the proposed algorithm is less observant for CW_{max} manipulations, the comparison of Figure 7a and 7b indicates the LOF progressively decreases and is more observant than local PDR values. Figure 11c also shows reduced throughput benefits for the cheating device.

2) One cheater per cell: Figure 11c does not show a considerable increase in average throughput of cheating stations. However, both NOF and PDR results in Figure 8 indicate variations that could indicate the presence of malicious stations. Being persistent, the objective function results follow a particular trend.



(a) LOF. (b) Local average PDR.

Fig. 7: One cheater in the network reducing CW_{max}.



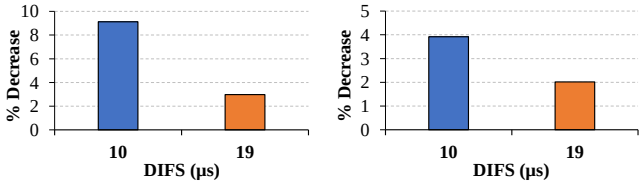
(a) NOF. (b) Average network PDR.

Fig. 8: One cheater per cell in the network reducing CW_{max}.

C. Cheaters with DIFS manipulations

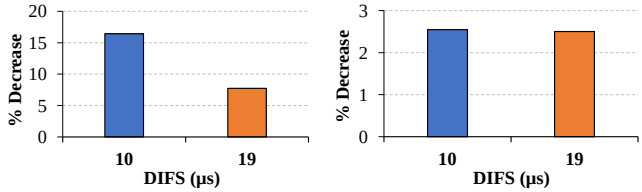
In the normal operations, the value of DIFS is set to the default value of 28 μs. A cheating device can be able to attain the access of the shared channel much more quickly if it can reduce its DIFS value. In this way, the cheater can prioritize its communication as compared to other stations. The smallest inter frame space used in IEEE 802.11 is the SIFS and its default value is 10 μs. The DIFS value for the cheater is decreased from 28 μs to 10 μs by changing the AIFSN value in Equation 2.

1) Single cheater in the network: Figure 9a indicates that the LOF value decreases when the cheater's DIFS is increased because having a large DIFS reduces its priority of channel access. For the cheater DIFS value of 10 μs, there is a more than 12% decrease in the objective function of the BSS. As indicated by Figure 9a, the LOF value for the particular case indicates almost 9% decrease in OBSS performance. As compared to Figure 9b, the objective function indicates significant variations. Figure 11e shows that by DIFS manipulations, the cheater can gain maximum benefits.



(a) LOF. (b) Local average PDR.

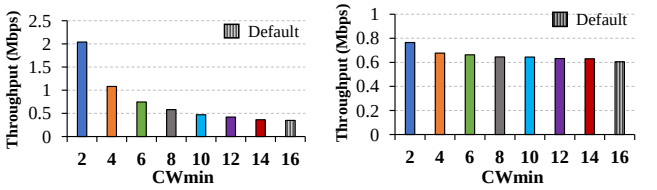
Fig. 9: One cheater in the network reducing DIFS.



(a) NOF. (b) Average network PDR.

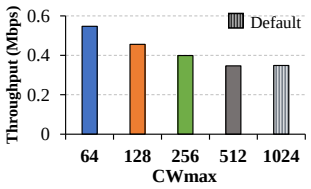
Fig. 10: One cheater per cell in the network reducing DIFS.

2) One cheater per cell: As indicated by Figure 11f, greater number is cheaters present in the network results in cheating stations competing among them selves and there is n considerable increase in average throughput of cheaters, Interestingly, as shown in Figure 10a, the NOF shows considerable decrease when compared with a system where every station performs normally. Also, the PDR values indicated in 10b are less significant.

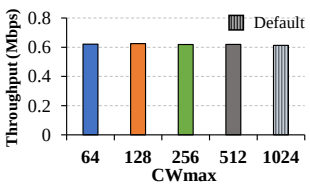


(a) One cheater reducing CW_{min}.

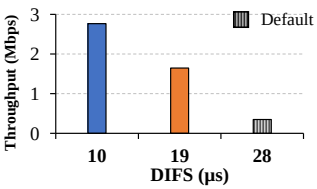
(b) One cheater per cell reducing CW_{min}.



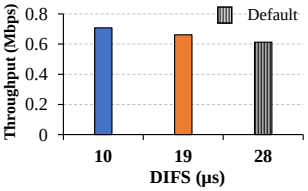
(c) One cheater reducing CW_{max}.



(d) One cheater per cell reducing CW_{max}.



(e) One cheater reducing DIFS.



(f) One cheater per cell reducing DIFS.

Fig. 11: Average throughput of cheater(s).

VI. Conclusion

The proliferation of IEEE 802.11 networks has made them an easy and attractive target for malicious devices to misuse the network. In this paper, we address the problem of detecting selfish stations in ultra dense Wi-Fi networks. A new detection mechanism based on an objective function is presented that uses per cell, neighboring cell and network wide statistics. While comparing the cheating strategies, the maximum variation in the objective function is seen for the case when the cheater is employing a decreased CW_{min}. However, maximum throughput benefits for the cheater was achieved when changing the DIFS value. Overall, the proposed scheme shows promising results in all cases. As compared to PDR based detection methods, our results show that this new mechanism is more sensitive. Future work includes development of analytical models (to provide a theoretical basis for the objective function heuristic presented in this paper), exploring the performance of the proposed scheme for the optional four-way handshake, and addressing the other cheater mechanisms. Moreover, the proposed mechanism would be enhanced to detect selfish/attacking APs within ultra dense network. There are also reasons to expect that this approach will work well for jammer detection.

Acknowledgements

This publication has emanated from research conducted with the financial support of Science Foundation Ireland (SFI) and is co-funded under the European Regional Development Fund under Grant Number 13/RC/2077. This work has been partially supported by the Spanish Ministry of Economy and Competitiveness and by the European Regional Development Fund under grant TEC2015-71303-R (MINECO/FEDER).

References

[1] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, "Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset," *IEEE Communications Surveys Tutorials*, vol. 18, no. 1, pp. 184–208, Firstquarter 2016.

[2] I. S. Association, "IEEE standard for information technology–telecommunications and information exchange between systems local and metropolitan area networks–specific requirements part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," *ANSI/IEEE Std. 802.11-2012*, 2012.

[3] P. Kyasanur and N. H. Vaidya, "Selfish mac layer misbehavior in wireless networks," *IEEE Transactions on Mobile Computing*, vol. 4, no. 5, pp. 502–516, Sept 2005.

[4] Z. Zhong, P. Kulkarni, F. Cao, Z. Fan, and S. Armour, "Issues and challenges in dense wifi networks," in *2015 International Wireless Communications and Mobile Computing Conference (IWCMC)*, Aug 2015, pp. 947–951.

[5] L. Guang, C. Assi, and A. Benslimane, "MAC layer misbehavior in wireless networks: challenges and solutions," *IEEE Wireless Communications*, vol. 15, no. 4, pp. 6–14, Aug 2008.

[6] M. Raya, I. Aad, J. P. Hubaux, and A. E. Fawal, "DOMINO: Detecting MAC layer greedy behavior in IEEE 802.11 Hotspots," *IEEE Transactions on Mobile Computing*, vol. 5, no. 12, pp. 1691–1705, Dec 2006.

[7] K. Pelechrinis, G. Yan, S. Eidenbenz, and S. V. Krishnamurthy, "Detecting selfish exploitation of carrier sensing in 802.11 networks," in *IEEE INFOCOM 2009*, April 2009, pp. 657–665.

[8] J. Tang, Y. Cheng, and W. Zhuang, "Real-time misbehavior detection in IEEE 802.11-Based Wireless Networks: An Analytical Approach," *IEEE Transactions on Mobile Computing*, vol. 13, no. 1, pp. 146–158, Jan 2014.

[9] E. Garcia-Villegas, M. S. Afaqui, and E. Lopez-Aguilera, "A novel cheater and jammer detection scheme for IEEE 802.11-based wireless LANs," *Computer Networks*, vol. 86, pp. 40 – 56, 2015.

[10] N. Kang, E. M. Shakshuki, and T. R. Sheltami, "Detecting misbehaving nodes in MANETs," in *Proceedings of the 12th International Conference on Information Integration and Web-based Applications & Services*, ser. iiWAS '10. ACM, 2010, pp. 216–222.

[11] S. Merlin, "IEEE 802.11 tgax simulation scenarios," *IEEE 802.11ax, IEEE 802.11-14/0621r3*.

[12] R. Jain, "Fairness: How to measure quantitatively?" *ATM Forum/94-0881, Sept. 1994*.

[13] M. S. Afaqui, S. Brown, and R. Farrell, "Uplink performance optimization of ultra dense Wi-Fi networks using AP-managed TPC," in *10th Wireless Days Conference*, April 2018, pp. 104–106.

[14] S. Zehl, N. Karowski, A. Zubow, and A. Wolisz, "Lows: A complete open source solution for wi-fi beacon stuffing based location-based services," in *2016 9th IFIP Wireless and Mobile Networking Conference (WMNC)*, July 2016, pp. 25–32.

[15] Hybrid buildings propagation loss model: ns3-design document. [Online]. Available: http://www.nsnam.org/docs/models/html/buildings-design.html

[16] M. S. Afaqui, E. Garcia-Villegas, and E. Lopez-Aguilera, "Dsc calibration results with ns-3," *IEEE 802.11ax, IEEE 802.11-15/1316-03-00ax*, November 2015.