International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 24 (2017) pp. 15409-15419

Achieving High Throughput and Fairness in Dense WLANs by Mitigating Problem Nodes

Irda Roslan[1], Takahiro Kawasaki[2], Toshiki Nishiue[3], Yumi Takaki[4], Chikara Ohta[5], Hisashi Tamaki[6]

[1-6] Graduate School of System Informatics, Kobe University, Rokkodai-cho 1–1, Nada-ku, Kobe, Hyogo 657–8501, Japan.

[1] Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Malaysia.

[1]Orcid: 0000-0002-5869-8187, [4]Orcid: 0000-0001-8277-092X, [5]Orcid: 0000-0002-4143-9429

Abstract

Hidden terminal and exposed terminal in wireless local area network are among the most common challenges that need to be handled whenever poor network performance is encountered. In a high dense wireless infrastructure environment, such terminal problems may result in deterioration of total network throughput due to high frame collisions and reduction of spatial reuse. Our proposed control scheme mitigates the hidden terminal and exposed terminal problems using carrier sense threshold tuning and transmit power control as well as enabling the RTS/CTS mechanism when necessary. These mitigation approaches take place once station identification are conducted where the membership of each neighboring stations are determined using Bloom filter method. The aim of this research is to assure that high total throughput of the network can be achieved while ensuring enhancement of throughput fairness for all stations. Our work also focuses on achieving higher minimum throughput for stations that suffers from extremely low throughput. We run a series of simulation experiment using IEEE 802.11g protocol in a network setup that imitates high dense environment and we managed to achieve better minimum throughput per station. This will give a good insight where the proposed control scheme can be potentially implemented in the high efficient wireless local area networks.

Keywords: IEEE 802.11; dense WLAN; carrier sense threshold; transmit power control; Bloom filter.

INTRODUCTION

The IEEE 802.11ax which is also known as High Efficiency Wireless LAN (HEW) is an amendment of IEEE 802.11 WLAN focusing on average throughput enhancement per STA while maintaining its power efficiency in high density environment [1]. This among others includes performance improvement of indoor deployment such as overcrowded apartments. Imagine a block of large apartment with hundreds of occupants where each house is installed with access points (APs). Each occupant has probably at least three devices such as smartphone, tablet PC and notebook. All these devices are preferable to be connected to the internet via WLAN so that the user can use them freely around the house. It may look convenient for the users to effortlessly checking emails, playing online games, watching on-demand videos and other services with the wireless network. These users however do not realize that there are many other occupants or neighbors living nearby who happened to deploy their own residence with AP as well. Let us assume that every residence has its own AP and the users are actively utilizing it. This would lead to massive problem of channel interferences from users' network that will badly affect each other to an extent where the aggregate network throughput deteriorates. This results in inconvenience and dissatisfaction among users in accessing the network.

To investigate this matter, we need to understand the nature of WLAN. Essentially, IEEE 802.11 WLAN is a wireless networking protocol that is widely used and commonly employ Distributed Coordination Function (DCF) mode of operation. DCF is based on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) that uses carrier sensing mechanism in determining the current status of medium channel. This medium channel is shared by all the stations (STAs) in the network where each and every one of them has equal opportunity to access it. Therefore, prior to frame transmission by any STA, the channel availability need to be determined first. This is done by measuring the amount of energy detected on the channel. If an STA detected the energy is above certain threshold, it will be aware that there is another STA out there currently accessing the channel. Realizing this, the STA will restrain itself from transmitting frame and stay still to avoid collisions.

Even though CSMA/CA functions well in avoiding frame collision, it still could not prevent the existence of hidden terminal and exposed terminal problems up to this day. In an infrastructure wireless environment, a hidden terminal occurs when an STA sends frame transmission to an AP without realizing there is another STA associated to the same AP sending frames to the AP as well. This happens when STAs are unable to detect the energy signal of each other and thus, are "hidden" from each other. When such situation occurs, frames at the AP side will continuously collide to an extent where packet loss ratio drops badly. Eventually, the aggregate throughput of the network degrades excessively.

To understand the exposed terminal problem, consider a scenario where there are two basic service sets (BSS) located next to each other. In each BSS, there is an STA associated to an AP. For instance in one BSS, STA 1 is associated to AP 1 while in another BSS, STA 2 is associated to AP 2. In such layout, there should be no problem for both STAs to transmit frames to

their respective AP. However, due to the adjacent location of both STAs, there is a possibility that interference happens where STA 1 could sense signals sent from STA 2 which is destined for AP 2. This has made STA 1 wrongfully assume that transmitting frame to AP 1 may cause collisions with frames coming from STA 2 which are actually not. Thus STA 1 decides to restrain itself from doing so and this results in decreasing number of spatial reuse. In such situation, we could say that both STAs are "exposed" to each other. The major problem caused by exposed terminal is the degradation of overall network throughput due to channel interferences that eventually lead to declining numbers of spatial reuse.

The massive number of exposed terminals in high dense WLAN environment will leave the network in bad performance as there are many "dead spots." This is where the poor STAs get the least minimum throughput and in worst case scenario, they could be denied from getting opportunity to access the medium channel. Thus we want to ensure that these STAs that suffer as exposed terminals will still get the chance to transmit frame by focusing on achieving higher minimum throughput per STA. To our knowledge, there is no other research works regarding mitigating exposed terminal problem aims to ensure that each affected STA achieves high minimum throughput in order to boost up the network performance. Ours will focus on this.

In this paper, we propose a control scheme that mitigates exposed terminal and hidden terminal by tuning carrier sense threshold (CST) and transmit power control (TPC) appropriately. It also applies RTS/CTS mechanism when necessary. With this proposed control scheme, an STA will first distinguishes the identity of adjacent STAs around it by applying the Bloom filter method [2]. By doing so, each STA is able to recognize STAs that are within the same BSS as it is and STAs that are not, and also detect the presence of STAs with potential terminal problems. The proposed control scheme then tunes the CST and TPC or even triggers RTS/CTS mechanism accordingly to alleviate exposed terminal and hidden terminal. Applying Bloom filter in the proposed control scheme helps to improve the overall network throughput as it reduces the overhead that is commonly arise in the standard 802.11 control scheme. The aim of our research is to achieve high total throughput of the network and ensure fairness enhancement among all STAs.

Our work in [3] evaluates the proposed control scheme on basic WLAN scenarios and compared it with the standard 802.11 scheme. Three different settings that represent low dense, medium dense and high dense networks are considered. In all scenario settings, our scheme managed to improve the total network throughput and gain better fairness. For this paper, we focus on evaluating the proposed control scheme to a more realistic scenario that represents dense WLAN where seven APs are associated with 42 STAs. These STAs are positioned randomly in their respective BSSs. Initially, we intended to run simulation experiments using IEEE 802.11ax (HEW) protocol. However the current deployment of HEW in the network simulator has not being released yet and thus IEEE 802.11g protocol is selected as it displays the most common WLAN environment. The detail explanation on the simulation setup can be found in Performance Evaluation section. We believe that the result of this simulation experiment will give positive overview where the proposed control scheme has good potential to be implemented in real dense IEEE 802.11ax (HEW) environment.

This paper is organized as follows: We start with explaining the common approaches used in mitigating hidden terminal and exposed terminal. This is followed by mentioning research works that are related to the mitigation approaches. Next, we explain how Bloom filter method is used in determining the membership of STAs prior to mitigation of both terminal problems. We then introduce our proposed control scheme which is followed by its performance evaluation. We finally wrap up our research work in the conclusion part.

HIDDEN TERMINAL AND EXPOSED TERMINAL MITIGATION APPROACH

Realizing the crucial problems of both hidden terminal and exposed terminal, there should be an effective mechanism that is able to deal with both of them either to mitigate completely or at least decreasing their effects. The trade-off of both terminal problems need to be considered well as excessively decreasing one will end up affecting the other. In general, there are three main approaches that are deployed in mitigating these problem terminals namely carrier sense threshold (CST), transmit power control (TPC) and Request to Send/Clear to Send (RTS/CTS) mechanism.

The IEEE 802.11 WLAN protocol uses DCF mode of operation that supports a common carrier sensing method namely Physical Carrier Sensing (PCS). Through PCS, an STA will determine the channel condition whether it is currently available to be accessed or not. The determination of the channel condition is done by sampling energy and it is then compared with a static value called carrier sense threshold (CST). If the received energy is less than the CST, the medium is considered as idle and the STA can access the channel by transmitting frames. Otherwise, the medium channel is in busy state and STA will refrain itself from sending frames. Basically CST can be tuned to mitigate both hidden terminal and exposed terminal. When CST of an STA is set to a low value, the PCS will become more sensitive and the STA's carrier sense range will be widen. This kind of setting is suitable to mitigate hidden terminal problem. On the other hand, a higher CST value will make PCS becomes less sensitive and thus the carrier sense range of the STA will become smaller. Exposed terminal problem can be alleviated using this method. Among previous works that focus on this CST adaptation are mentioned in [4, 5, 6, 7].

The second approach that is also commonly used is utilizing transmit power control (TPC) [9, 10, 11]. When a target STA is identified as a hidden terminal, the TPC of the focused STA can be increased so that the energy could be heard by the STA and thus eliminate hidden terminal problem. Transmission power can also be decreased to avoid channel interferences among STAs and eventually prevent exposed terminal from occurring.

The adaptation of TPC however needs to be handled cautiously as over increasing it will lead to severe channel interferences in the network and setting it to a very low value will degrade the overall network throughput.

RTS/CTS is an optional mechanism used by the IEEE 802.11 WLAN protocol to reduce frame collisions that are caused by hidden terminal. It uses another type of carrier sensing method in CSMA/CA which is the virtual carrier sensing (VCS). The RTS/CTS is initiated to fix the hidden terminal problems that can appear in PCS used by the 802.11 WLAN protocol. This mechanism unfortunately does not solve the exposed terminal problem. The performance evaluation of RTS/CTS mechanism can be found in [12, 13]. The RTS/CTS mechanism however is only suitable for long sized packet. Enabling RTS/CTS for short packets may cause overhead. Research works focusing on mitigating hidden terminal and exposed terminal using these three approaches are explained in detail in the following section.

RELATED WORKS

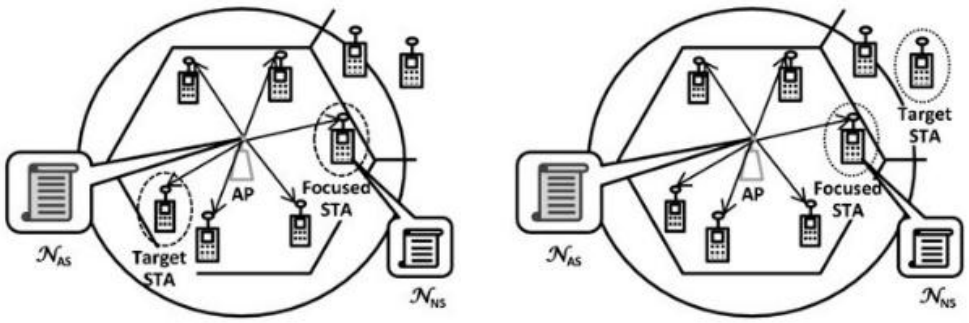
In [7] the authors proved that the aggregate throughput of dense WLAN focusing on IEEE 802.11n can be improved with CST adaptation. This is achieved by ensuring that optimized solutions are taken into account in terms of data rate, access method and coexistence with legacy devices. Some guidelines related to the CST adaptation are also recommended in order to enhance the capacity of WLAN network. In another work [8], the same authors introduce an algorithm that allows CST to be adapted dynamically. This CST adaptation scheme mitigates hidden terminal and exposed terminal in attempt to achieve high network throughput by considering the use of margin value. This margin value needs to be set so that it covers the hidden node region sufficiently without further presence of exposed node to increase spatial reuse. Despite of focusing on getting high spatial reuse, these schemes however do not guarantee throughput fairness of all STAs in the network.

In order to improve efficiency of high dense WLAN environment, [14] evaluates carrier sensing amendments recommended by the IEEE802.11ax (HEW) protocol. The Dynamic Sensitivity Control (DSC) algorithm has been introduced where it employs CST adaptation based on average received signal strength. It is expected that the DSC algorithm is able to escalate the number of concurrent transmissions. This is conducted in a distributed manner where each STA tunes its own CST based on the channel conditions and received power. Even though this algorithm managed to achieve high throughput and fairness, the network still suffers from increasing numbers of hidden terminals as well as high frame error rate (FER).

On the other hand, [10] emphasizes on the use of TPC technique. Fractional CSMA has been proposed which combines enhanced TPC, user grouping and inter-BSS coordination with the aim of achieving maximum throughput and energy efficiency. There is no CST adaptation incorporated in this scheme. Even though high throughput can be gained in dense and overlapped network via simulation, the practicality of this scheme can be disputed as PHY layer modification needs to be done in each STAs in the network.

There are also some problem terminal mitigation schemes that suggested the adaptations of several network parameters which are simply known as joint tuning method. A joint tuning scheme of CST, TPC and data rate has been proposed by [15] in an attempt of achieving high total throughput and fairness improvement in high density WLAN. To achieve this, an analytical model is introduced where two adaptation rules are proposed. The first rule is to balance CST and TPC by ensuring the product of both parameters is equivalent to a fixed constant. Whereas the second rule emphasizes on achieving time-sharing fairness among all STAs. Depending on these rules, the proposed joint tuning scheme is conducted in distributed manner where the adaptation is done by the STAs themselves.

A joint tuning of TPC and CST scheme based on diff erentiated packet error rate (PER) is proposed by [16] to improve spatial reuse in dense WLAN environment. With this scheme, each STA tunes its own parameters using its own local measurements in order to mitigate interference. By doing so, the overhead that resulted from common information changing can be refrained. Although both of these joint tuning schemes guarantee fairness at all STAs in the WLAN, they still have shortcomings in identifying which of the neighboring STAs are problem terminals and which are not.



(a) Identifying hidden terminal (b) Identifying exposed terminal

Figure 1: Identifying hidden terminal and exposed terminal in WLAN

DETERMINE MEMBERSHIP OF STAS USING BLOOM FILTER

In a high dense wireless environment that is overcrowded with massive numbers of STAs, the aggregate throughput as well as concurrent transmissions in the network tend to be badly deteriorated due to hidden terminals and exposed terminals. Hence, there is a need of a mechanism that allows each STA to identify the existence of hidden terminal and exposed terminal from its own perspective among its neighboring STAs. Subsequently, the problem terminals can be dealt correspondingly. Thus, our basic idea is to find an effective way to accomplish this by identifying whether the neighboring STAs are located within the same BSS as the target STA or not. This could be done by checking the membership of the neighboring STAs using Bloom filter approach.

Figure 1 shows a simple approach that could be applied in identifying hidden terminal and exposed terminal. In a BSS, an AP keeps a list, $\mathcal{N}_{AS}$, of associated and pseudo-associated STA identifications (ID). Pseudo-associated STA refers to an STA that belongs to other BSS but its signal can be sensed by the AP at the current BSS. Besides AP, each and every STA also keeps its own local list, $\mathcal{N}_{NS}$, of neighboring STA IDs. For STA identification purpose, AP broadcasts the list that it keeps to all STAs in its BSS. Upon receiving it, a focused STA (STA who does the membership checking) will compare the list received from AP with its own list. Referring to Fig. 1a, if the target STA (STA that is being checked) exists in AP's list but not in the focused STA's list, then this target STA is indeed a hidden terminal to the focused STA. On contrary, if the target STA exists in the focused STA's list but not in the received AP's list, the target STA is considered as exposed terminal to the focused STA as shown in Fig. 1b. We could simply use this method of identifying the STAs in our proposed control scheme. However, in dense WLAN environment where the BSSs are overcrowded with STAs, using this method of broadcasting the lists via control frames may cause overhead. This is due to the fact that AP needs to maintain a list of large numbers of STAs and broadcast larger frame size to all STAs.

As a solution to this matter, we introduce the use of Bloom filter to check the membership status of neighboring STAs. Basically Bloom filter is a simple and space-efficient data structure for testing membership of an element in a set of elements. It is introduced by Burton Bloom [2] in the 1970s and is widely applied in many applications including web searching, databases and computer network applications [17].

The Bloom filter comprises of an array of m bits, that represents a set $\mathcal{S} = \{i_1, i_2, ..., i_n\}$ of n elements. Initially, all of the m bits in the array is set to 0. Everytime an element is added to the bit array, it will be hashed k times where k refers to independent hash functions $h_1, ..., h_k$. Each hash yields a bit location which are then mapped to a random uniform over the range $\{1, ..., m\}$. Whenever an element is hashed, the respective bits are set to 1. To check the membership of an element whether it is in the set of elements or not, it is hashed k times and the resulting bits are checked for a match. If there is a 0 found in the corresponding bit, then the element cannot be in the set. If it matches with all 1s, that particular element is either in the set or the filter probably returns a false positive result [18].

False positive refers to a case where a false match of a non-element member can be found in the bit array. This indicates that an element is either probably in the set or definitely not in the set. Though false positive might appear in Bloom filter, it is absolutely free from false negative result. The details on the false positive probability are mentioned in [18].

For our proposed control scheme, the Bloom filter is used to insert new STA IDs in the set or to find a match of STA ID that exists in the set for identification purpose. The i element in the Bloom filter represents the ID of STAs. This means for $\mathcal{N}_{AS}$, the set contains the IDs of associated and pseudo-associated STAs of an AP. As for $\mathcal{N}_{NS}$, the set contains the IDs of neighboring STAs of a focused STA. If there happens to be a false positive, the STA ID could be falsely found in the set. However, there will be no cases of false negative where an STA ID that is added to the set earlier could not be found in the set. Therefore, we need to set the false positive probability as small as possible to ensure Bloom filter works well in identifying the membership of STAs. In calculating false positive, the parameters that are taken into account include number of element bits in array m, hash function k and number of inserted elements n, i.e. the number of STA IDs. To obtain small probability of false positive, the value of m should be increased. Increasing n on the other hand will increase the probability of false positive. Thus, to satisfy let say 0.001 false positive probabilities, the value of k should be at least 10 and if n is 100, the value of m should be set to 1,400. We set these values in our proposed control scheme. In the next section, we explain how Bloom filter is applied in the proposed control scheme as well as the detail procedure of exposed terminal and hidden terminal mitigation.

PROPOSED CONTROL SCHEME

As mentioned earlier, the objective of our research is to achieve high total throughput and ensure all STAs receive better throughput fairness especially in the condition of high density WLAN. STAs that suffer from low throughput due to exposed terminal problem are also ensured to gain higher minimum throughput. To accomplish this, our proposed control scheme suggests the adjustment of preamble detection threshold P_{PD} (carrier sense threshold) and transmission power P_{TX} to mitigate hidden terminal and exposed terminal problems. The scheme also enables the use of RTS/CTS mechanism if necessary in the case of solving hidden terminal problem. For ease of understanding, the meanings of the notation used here onwards can be referred to Table 1.

Table 1: Notations and Meanings for the Proposed Control Scheme.

Notation	Meaning
$\mathcal{N}_{AS}$	A set of associated and pseudo-associated STAs of an AP
N_{AS}	The number of elements in $\mathcal{N}_{AS}$ ($\mid \mathcal{N}_{AS} \mid$)
$\mathcal{N}_{NS}$	A set of neighboring STAs of a focused STA
N_{HS}	The number of hidden STAs of a focused STA
$\mathcal{N}_{ES}$	A set of exposed STAs of a focused STA ($\mathcal{N}_{NS} \setminus \mathcal{N}_{AS}$)
N_{ES}	The number of exposed STAs of a focused STA
P_{PD}	Preamble detection threshold
P_{PD}^{min}	Minimum preamble detection threshold
P_{PD}^{tmp}	Temporal variable to determine P_{PD}
P_{PD}^{max}	Maximum P_{PD} value allowed
P_{PD}^{inc}	Preamble detection threshold increment value
P_{PD}^{dec}	Preamble detection threshold decrement value
P_{TX}	Transmission power of focused STA
P_{TX}^{max}	Maximum transmission power
P_{TX}^{limit}	P_{TX} upper limit
P_{TX}^{inc}	P_{TX} increment value
P_{TX}^{dec}	P_{TX} decrement value
$P_{RX\_AS}^{min}$	Minimum power reception from STA in $\mathcal{N}_{AS}$
$P_{RX\_AS\_far}^{min}$	P_{TX} based on minimum reception power for farthest STA
$P_{RX\_AS\_far}^{max}$	P_{TX} based on maximum reception power for farthest STA
$P_{RX\_ES}^{min}$	Minimum reception power from STA in $\mathcal{N}_{ES}$
$P_{RX\_ES}^{inc}$	P_{RX_ES} increment value
P_{RX_AP}	Reception power of AP associated by a focused STA
$P_{RX\_AP}^{dec}$	P_{RX_AP} decrement value
N_{RL}	Retransmission retry limit
t	Waiting time

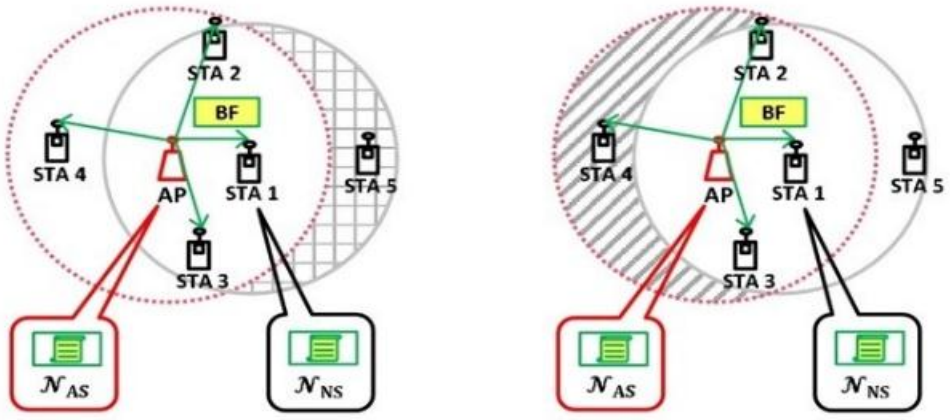
The proposed control scheme is initiated by accomplishing STA identification where Bloom filter is utilized to check STA's membership as explained in Section 4. For every BSS, each of the STA keeps a list of neighboring STA IDs ($\mathcal{N}_{NS}$) while AP maintains a list of associated STAs and pseudo-associated STA IDs ($\mathcal{N}_{AS}$). AP will broadcast the list that it maintains including the number $\mathcal{N}_{AS}$ of STAs ($|\mathcal{N}_{AS}|$) to all STAs associated to it using control frame which is called Bloom filter frame. After focused STA determines the identity of the target STA, the scheme will react accordingly with the parameter tunings when the target STA is found to be hidden terminal or exposed terminal.

To understand how STAs conduct membership checking and mitigate exposed terminal or hidden terminal accordingly using the proposed control scheme, refer to Fig. 2. Consider a scenario where there are four STAs (STA 1 to STA 4) associated to an AP in a BSS while another STA (STA 5) belongs to the other BSS. The dotted circle represents the carrier sense range of the AP while the solid circle represents the carrier sense range of STA 1. Let STA 1 be the focused STA that will do membership checking of all other neighboring STAs. Once STA 1 receives Bloom filter frame that is broadcasted by the AP, it will compare the list of STAs ($\mathcal{N}_{AS}$) maintained by the AP which includes the number of STAs, with the list ($\mathcal{N}_{NS}$) that it maintains locally.

The STAs that exist in both lists in Fig. 2 are as follows; $\mathcal{N}_{AS} = \{1, 2, 3, 4\}$ and $\mathcal{N}_{NS1} = \{1, 2, 3, 5\}$.

For the case of mitigating exposed terminal, the focused STA detected exposed terminal when there is an STA appears in its own list but not in the AP's list. As shown in Fig. 2a, STA 1 detected that there is STA 5 in its own list but not in AP's list as appeared in the checkered area. Thus STA 1 identified STA 5 as exposed terminal. Upon detecting an exposed terminal, STA 1 will increase its carrier sense threshold to shorten its carrier sense range. The threshold increment is done gradually to an extent where it is higher than the current preamble threshold but still lower than the minimum reception power of all STAs in $\mathcal{N}_{AS}$. This is to ensure that the exposed terminal can be mitigated without causing the appearance of hidden terminal. The transmission power of STA 1 is also decreased if it is found to be too high.

Figure 2b on the other hand shows how hidden terminal is detected and alleviated. Focused STA sensed the presence of a hidden terminal when there is an STA appears in the AP's list but not in its own list. In this example, STA 1 detected that STA 4 is the hidden terminal when STA 4 exists in the AP's list but not in its own list as depicted by the stripe area. To deal with hidden terminal, STA 1 checks itself whether its own carrier sense range can be widen or not. If it is possible, STA 1 reduces the preamble detection threshold. If it is not possible due to the minimum value of preamble detection threshold, the RTS/CTS mechanism is triggered for frames of 1,000 octets or more. Enabling RTS/CTS mechanism for frames that are less than the stated threshold will cause overhead due to inefficient changings of RTS/CTS control frames. This will lead to poor wireless network performance.



(a) Mitigate exposed terminal (b) Mitigate hidden terminal

Figure 2: Mitigating exposed terminal and hidden terminal using the proposed control scheme

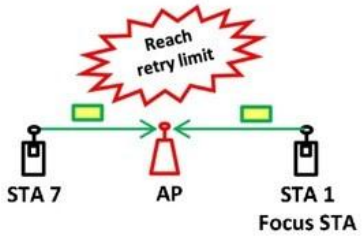


Figure 3: Focused STA itself is the hidden terminal

Our proposed control scheme also introduces mitigation mechanism when the focused STA finds that itself is the hidden terminal. This is as shown in Fig. 3. Consider when the focused STA (STA 1) is transmitting a frame to the AP. The frame is however dropped at the AP's side. When this happens, STA 1 retransmits the frame to the AP and the frame keeps dropping out by the time it arrives at the AP's side. This happens repeatedly until retry limit has been reached. Realizing this, STA 1 knows that it is indeed is the hidden terminal to the other terminal out there (STA 7). What actually happens is frame collisions occur between frames transmitted by both STA 1 and STA 7 at the AP's side which caused dropping of frames from both sides. At this level, the frame error rate (FER) for both STAs increase and might results in low network throughput. Therefore, STA 1 increases its transmission power gradually until its signal can be sensed by STA 7.

The procedure of the proposed control scheme is as shown in Fig. 4 where we alleviate the exposed terminal first and followed by hidden terminal. Managing the control scheme with such approach boosts the network performance as more spatial reuse among STAs can be granted and eventually higher aggregate throughput can be achieved.

The following is the procedure of the proposed control scheme:

1. When waiting time expires in a focused STA, the STA will compare $\mathcal{N}_{AS}$ contained in Bloom filter frame that is retrieved from AP with $\mathcal{N}_{NS}$ in its list.
2. If an STA in $\mathcal{N}_{NS}$ does not match with $\mathcal{N}_{AS}$, it is considered as an exposed terminal and is listed in the exposed STA list, $\mathcal{N}_{ES}$.
3. To mitigate exposed terminal problem, P_{PD} needs to be increased to reduce carrier sense range and/or P_{TX} needs to be decreased. To do so, first the minimum reception power $P_{RX\_ES}^{min}$ from exposed STAs in $\mathcal{N}_{ES}$ is determined. Then temporal variable P_{PD}^{tmp} is set and will then updated to P_{PD} if some conditions are satisfied.
4. The value of P_{PD}^{tmp} should be greater than P_{PD} and should not be larger than the allowable preamble detection threshold, P_{PD}^{max}.
5. If P_{PD}^{tmp} is higher than $P_{RX\_AS}^{min}$, it will cause more hidden terminals in $\mathcal{N}_{AS}$ from the viewpoint of the focused STA. In such case, P_{PD}^{tmp} is ignored.
6. To ensure downlink communication, P_{PD} should not be close to P_{RX_AP} and thus the transmission power value is decreased by $P_{RX\_AP}^{dec}$.

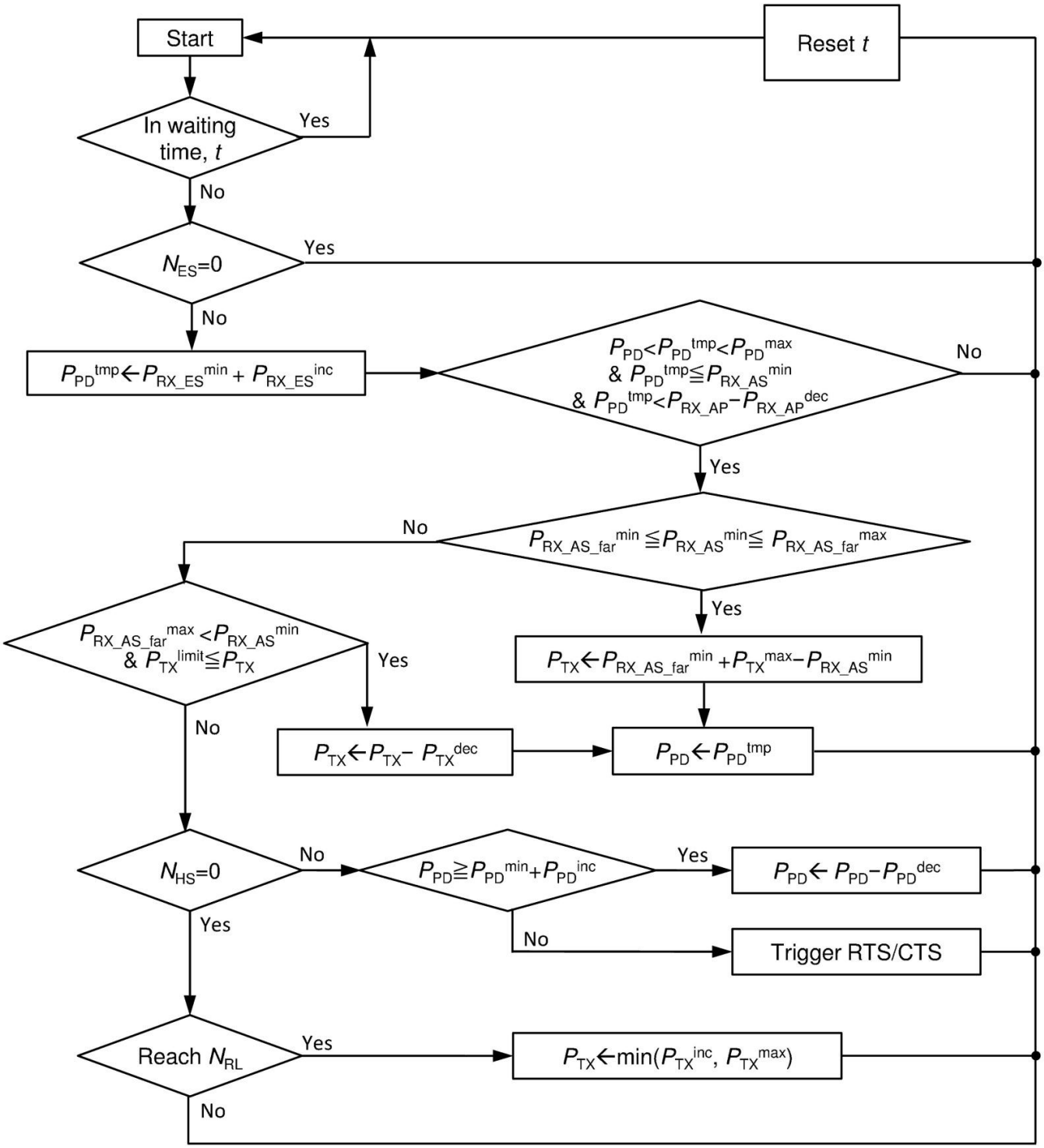


Figure 4: Flowchart of the proposed control scheme

7. The focused STA estimates the path loss between itself and the farthest STA in $\mathcal{N}_{AS}$ based on $P_{RX\_AS}^{min}$ and implicit assumption that the farthest STA transmits at the maximum power P_{TX}^{max}. And then P_{TX} is tuned so that the farthest terminal could receive the least minimum reception, $P_{RX\_AS\_far}^{min}$ if $P_{RX\_AS\_far}^{min} \leq P_{RX\_AS}^{min} \leq P_{RX\_AS\_far}^{max}$.
8. If the current P_{TX} is higher than P_{TX}^{limit} and $P_{RX\_AS}^{min}$ is more than $P_{RX\_AS\_far}^{max}$, the P_{TX} will be decreased by P_{TX}^{dec}.
9. The value of P_{PD} is updated as $P_{PD} \leftarrow P_{PD}^{tmp}$.
10. If hidden terminals exists when comparing $\mathcal{N}_{NS}$ and $\mathcal{N}_{AS}$, i.e. $N_{HS} > 0$, the preamble detection threshold will be reduced to increase the carrier sense range and P_{PD} will be

updated.

11. If P_{PD} could not be decreased owing to P_{PD}^{min}, the RTS/CTS mechanism will be triggered.
12. If the focused STA retransmits frames up to N_{RL} times, which will cause frame drops, it assumes that itself is the hidden terminal from the viewpoint of other STA. Therefore, the focused STA will increase P_{TX} so that it can be sensed by others.
13. The focused STA will reset its waiting time, *t*.

For the evaluation of the proposed control scheme, we set some values on certain parameters as found in Table 2. In next section, the details of the performance evaluation are discussed.

Table 2: Values set for the proposed control scheme.

Notation	Values
P_{PD}^{max}	-75 dBm
P_{PD}^{inc}	2 dB
P_{PD}^{dec}	2 dB
P_{TX}^{max}	20 dBm
P_{TX}^{limit}	15 dBm
P_{TX}^{inc}	1 dB
P_{TX}^{dec}	5 dB
$P_{RX\_AS\_far}^{min}$	-72 dBm
$P_{RX\_AS\_far}^{max}$	-67 dBm
$P_{RX\_ES}^{inc}$	1 dB
$P_{RX\_AP}^{dec}$	5 dB
t	100 ms

PERFORMANCE EVALUATION

To represent dense WLAN environment, we conducted a simulation of seven APs associated with 42 STAs. The layout of the network is as depicted in Fig. 5 where each BSS is represented by a hexagon that consists of an AP associated with six randomly positioned STAs. The STAs here are represented by squares. The BSSs are located next to each other where a wall is installed at the adjacent side of each BSS.

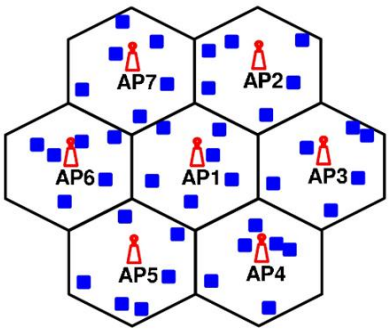


Figure 5: Random position of STAs in 7 APs scenario

To evaluate the effectiveness of the proposed control scheme, we set 20 different random position patterns for all the 42 STAs. For each set of pattern we run 10 trials of simulation. The simulation is conducted using Scenargie [19], a commercial simulator and the parameter settings are as listed in Table 3. In the current Scenargie simulation deployment, the IEEE 802.11ax (HEW) protocol has not being released yet and thus we set the scenario to run in 802.11g protocol which portrays the most common WLAN environment.

Table 3: Simulation settings.

Item	Value
Simulator	Scenargie 2.0
Simulation time	100 s
Simulation trials	10
MAC protocol	IEEE 802.11g
Rate adaptation	Minstrel
Pathloss model	COST231 Indoor
Traffic model	VBR
Default Tx Power	20 dBm
Default preamble threshold	-82 dBm
Size of a packet	128 bytes
Offered load	2 Mbit/s
Bit array, *m*	1400
Hash function, *k*	10
Number of STA IDs inserted, *n*	100

We evaluated the performance of the proposed control scheme and compared it with the standard 802.11 scheme in terms of the total throughput of the network, the fairness of STAs in getting adequate throughput and the minimum throughput that can be achieved by an STA. For this purpose, 2 Mbit/s of traffic loads are used to examine the trend of the results.

To obtain the fairness of STAs, the Jain's fairness index, *F*, is used which is given by $F = (\sum_{i=1}^{n} x_i)^2 / (n\sum_{i=1}^{n} x_i^2)$, where n is the number of STA and x_i is the throughput of each STA i [20]. The range of the fairness index is between zero and one. When the fairness index is closer to one, the STA obtains high throughput fairness and vice versa. We want to figure out whether all the STAs manage to achieve high fairness by observing the average fairness index for both schemes.

In dense WLAN, problem terminals especially the exposed terminals tend to receive very low throughput as they failed to get adequate opportunities to access the channel. The increasing number of exposed terminals notably at the edge of adjacent BSSs makes these areas susceptible to "dead spots".

Hence, we want to examine whether the proposed control

scheme is able to handle this issue by ensuring each STA gains better minimum throughput as we emphasized in the Introduction section. This in a way ratify that STAs indeed achieve high fairness.

Table 4 shows the performance evaluation results for all 42 STAs where the simulation has been set to run with 20 different sets of pattern. We compare the performance of the proposed control scheme (represented by Proposed) with the standard 802.11 scheme (represented by Standard) on three different measures which are the average throughput, fairness index and minimum throughput gained by each STA.

Table 4: Performance evaluation results for 20 different set of patterns.

Pattern	Average Throughput [Mbit/s]		Fairness Index		Min Throughput per STA [Mbit/s]	
	Std	Prop	Std	Prop	Std	Prop
1	31.83	32.56	0.64	0.76	0.06	0.12
2	31.62	32.77	0.66	0.76	0.12	0.14
3	32.39	32.17	0.66	0.78	0.03	0.10
4	32.99	33.53	0.61	0.71	0.04	0.02
5	31.49	32.31	0.67	0.77	0.05	0.03
6	31.47	32.51	0.69	0.81	0.14	0.01
7	31.45	32.33	0.60	0.80	0.07	0.01
8	30.12	31.38	0.60	0.71	0.07	0.10
9	32.99	32.86	0.64	0.82	0.04	0.08
10	31.49	31.77	0.62	0.76	0.05	0.16
11	31.23	32.24	0.66	0.81	0.10	0.11
12	32.23	32.19	0.66	0.78	0.10	0.05
13	31.81	32.57	0.64	0.74	0.06	0.06
14	32.89	32.90	0.69	0.84	0.07	0.15
15	29.14	31.03	0.60	0.70	0.14	0.08
16	32.51	32.59	0.72	0.80	0.10	0.09
17	31.78	33.11	0.65	0.78	0.09	0.12
18	29.02	31.45	0.60	0.74	0.08	0.16
19	32.65	32.95	0.66	0.77	0.04	0.14
20	32.34	32.20	0.68	0.81	0.12	0.09

Std – Standard 802.11 scheme
Prop – Proposed control scheme

The proposed control scheme managed to achieve higher average throughput at 16 patterns from the total set of patterns. While the standard scheme achieve higher average throughput at the remaining patterns (Pattern 3, 9, 12 and 20). This means that the proposed control scheme produces better average throughput at most scenarios and hence contribute to better network performance in dense environment WLAN.

As for fairness index, the proposed scheme achieved higher fairness at all patterns by obtaining index values higher than 0.70. This indicates that most STAs receive satisfactory throughput even for STAs that are considered as exposed terminals. To observe how each and every STAs receive throughput fairness, we combined a total of 840 throughputs which are obtained from these 20 different patterns. The Cumulative Distribution Function (CDF) of the average total throughput is generated as shown in Fig. 6. STAs achieve absolute fairness when vertical straight line of graph is generated which indicates that all of the STAs receive absolute high throughput. From the simulation result, the graph line of the proposed control scheme is closer to vertical line compared to the standard scheme. This implies that the proposed control scheme exhibits better fairness with 60% of the STAs achieved higher average throughputs even in low traffic loads.

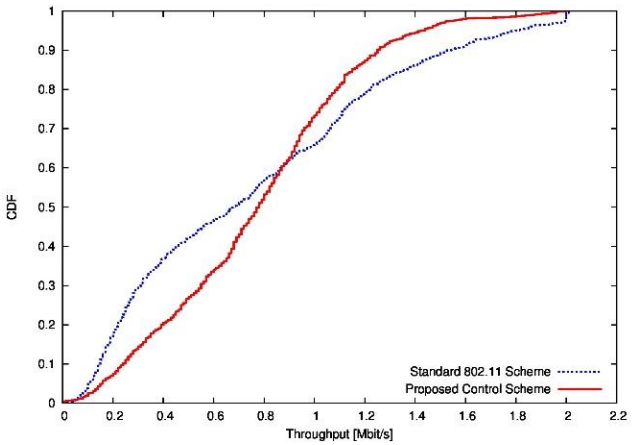


Figure 6: CDF for 840 throughputs (42 STAs run in 20 trials)

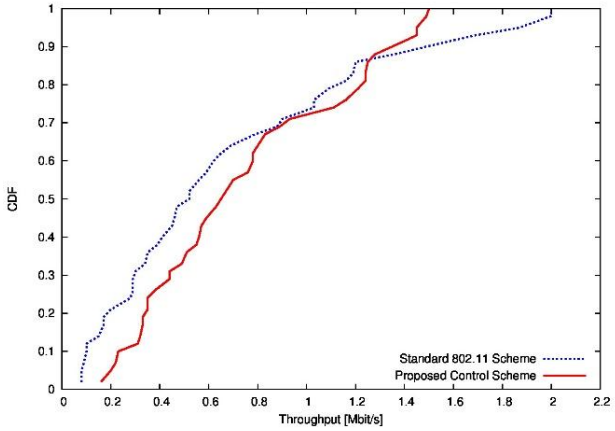


Figure 7: Pattern 18 which results in high minimum throughput for proposed control scheme

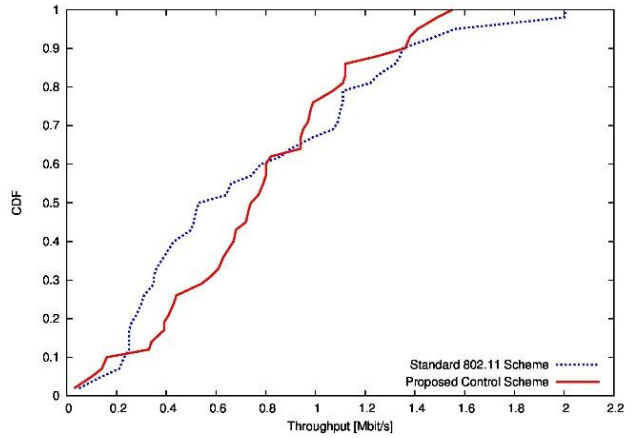


Figure 8: Pattern 5 which results in low minimum throughput for proposed control scheme

Next, we want to determine which of these schemes produce higher throughput for an STA that receives the least throughput in the network. From all 20 set of patterns, the proposed control scheme managed to obtain better minimum throughput per STA at 12 patterns. From our observation, in most set of patterns, the STA with the least throughput in proposed control scheme shows better enhancement than the standard scheme. The example of this scenario can be seen in Pattern 18 shown in Fig. 7. Almost 70% of the STAs consistently gained better throughput improvement as compared to the standard scheme. There are also some scenarios where minimum throughput gained by the standard scheme exceeds the one earned by the proposed control scheme. An example of this scenario can be seen in the case of Pattern 5 shown in Fig. 8. Even though the proposed control scheme does not dominate higher minimum throughput per STA at all set of patterns, the average total throughput achieved by the proposed control scheme is still remarkable with 32.37 Mbit/s compared to the standard scheme that achieves only 31.67 Mbit/s (refer to Table 5).

Table 5 summarizes the performance evaluation results of both standard scheme and proposed control scheme. As shown in the table, besides excel in earning higher average total throughput, the proposed control scheme improves fairness index with 18.5% increment as well as gaining about 16% improvement on minimum throughput per STA. In overall, the proposed control scheme delivers very promising outcome as it is able to outperform standard 802.11 scheme based on the measures used for evaluation.

Table 5: Summary of performance evaluation results.

Scheme	Average Total Throughput [Mbit/s]	Fairness Index	Minimum Throughput per STA [Mbit/s]
Standard	31.67	0.65	0.078
Proposed	32.37	0.77	0.091

CONCLUSION

In mitigating exposed terminal and hidden terminal problem in high dense WLAN, our proposed control scheme tunes CST and TPC appropriately. The RTS/CTS mechanism is also enabled if necessary. The enhancement in the network performance could be achieved due to the deployment of Bloom filter method for STA identification in the proposed control scheme. As a result, common overhead received when AP broadcasts large packet size to associated STAs could be reduced and thus high total throughput could be obtained. The evaluation of the proposed control scheme in a scenario that imitates high density WLAN shows that high total throughput can be achieved, the fairness of throughput among all STAs are enhanced as well as better minimum throughput are gained per STA. It is expected that the similar positive patterns of result could be achieved when the exact IEEE 802.11ax (High Efficiency WLAN) protocol is implemented. The same result patterns should be obtained when the simulation scenario are increased with enormous number of APs and STAs.

ACKNOWLEDGEMENT

This work was supported by JSPS KAKENHI Grant Numbers 15K00124 and 15K00125.

REFERENCES

[1] 802.11.ax Project Authorization (PAR) document, https://mentor.ieee.org/802.11/dcn/14/ 11-14-0165-01-0hew-802-11-hew-sg-proposed-par.docx, 2014 (accessed on 18.04.2016).

[2] Bloom, B. H., 1970, "Space/Time Trade-Offs in Hash Coding with Allowable Errors", Communications of the ACM, pp.422–426.

[3] Roslan, I., Kawasaki, T., Nishiue, T., Takaki, Y., Ohta, C., and Tamaki, H., 2016, "Control of Transmission Power and Carrier Sense Threshold to Enhance Throughput and Fairness for Dense WLANs", ICOIN 2016, Sabah, Malaysia, pp.51–56.

[4] Thorpe, C., and Murphy, L., 2014, "A Survey of Adaptive Carrier Sensing Mechanisms for IEEE 802.11 Wireless Networks", IEEE Comm. Surveys & Tutorials, 16 (3), pp.1266–1293.

[5] Haghani, E., Krishnan, M. N., and Zakhor, A., 2010, "Adaptive Carrier-Sensing for Throughput Improvement in IEEE 802.11 Networks", Proc. IEEE GLOBECOM 2010, Miami, FL, USA, pp.1–6.

[6] Thorpe, C., Murphy, S., and Murphy, L., 2011, "IEEE802. 11k Enabled Adaptive Carrier Sense Management Mechanism (KAPCS2)", Proc. IFIP/IEEE International Symposium on Integrated Network Management, Dublin, Ireland, pp.509–515.

[7] Jamil, I., Cariou, L., and Helard, J. F., 2014, "Improving the Capacity of Future IEEE 802.11 High Efficiency

WLANs", Proc. IEEE ICT2014, Lisbon, Portugal, pp.303–307.

[8] Jamil, I., Cariou, L., and Helard, J. F., 2015, "Efficient MAC Protocols Optimization for Future High Density WLANs", WCNC 2015, New Orleans, LA, USA, pp.1054–1059.

[9] Qiao, D., Choi, S., and Shin, K. G., 2007, "Interference Analysis and Transmit Power Control in IEEE 802.11 a/h Wireless LANs", IEEE/ACM Trans. on Networking, 15 (5) pp.1007–1020.

[10] Oteri, O., Xia, P., LaSita, F., and Olesen, R., 2013, "Advanced Power Control Techniques for Interference Mitigation in Dense 802.11 Networks", WPMC 2013, New Jersey, USA, pp.1–7.

[11] Zhou, Y., and Nettles, S. M., 2005, "Balancing The Hidden And Exposed Node Problems With Power Control In CSMA/CA-Based Wireless Networks", Proc. IEEE WCNC2005, New Orleans, LA, USA, 2 pp.683–688.

[12] Jasani, H., and Alaraje, N., 2007, "Evaluating the Performance of IEEE 802.11 Network Using RTS/CTS Mechanism", Proc. IEEE International Conference on Electro/Information Technology, Chicago, IL, USA, pp.616–621.

[13] Boroumand, L., Khokhar, R. H., Bakhtiar, L. A., and Pourvahab, M., 2012, "A Review of Techniques to Resolve the Hidden Node Problem in Wireless Networks", Smart Computing Review, 2 (2), pp.95–110.

[14] Afaqui, M. S., Garcia-Villegas, E., Lopez-Aguilera, E., Smith, G., and Camps, D., 2015, "Evaluation of Dynamic Sensitivity Control Algorithm for IEEE 802.11ax", WCNC 2015, New Orleans, LA, USA, pp.1060–1065.

[15] Zhou, Z., Zhu, Y., Niu, Z., and Zhu, J., 2007, "Joint Tuning of Physical Carrier Sensing, Power and Rate in High-Density WLAN", APCC 2007, Bangkok, Thailand, pp.131-134.

[16] Ma, H., Zhu, J., Roy, S., and Shin, S. Y., 2008, "Joint Transmit Power And Physical Carrier Sensing Adaptation Based On Loss Diff erentiation For High Density IEEE 802.11 WLAN", Computer Networks, 52 (9), pp.1703–1720.

[17] Blustein, J., and El-Maazawi, A., 2002, "Bloom filters. A Tutorial, Analysis, And Survey", Technical Report CS-2002-10, Dalhousie University, pp.1–31.

[18] Broder, A., and Mitzenmacher, M., 2004, "Network Applications of Bloom filters: A Survey", Internet Mathematics, 1 (4), pp.485–509.

[19] Scenargie, http://www.spacetime-eng.com/en/, (accessed on 8.7.2015).

[20] Jain, R., Chiu, D. M., and Hawe, W., 1984, "A Quantitative Measure Of Fairness And Discrimination For Resource Allocation In Shared Computer Systems", DEC Research Report TR-301.