Power interference modeling for CSMA/CA based networks using directional antenna

Saravanan Kandasamy [a,b,*], Ricardo Morla [a,b], Manuel Ricardo [a,b]

[a] Centre for Telecommunications and Multimedia, INESC TEC, Porto, Portugal
[b] Faculty of Engineering, University of Porto, Portugal

ABSTRACT

In IEEE 802.11 based wireless networks adding more access points does not always guarantee an increase of network capacity. In some cases, additional access points may contribute to degrade the aggregated network throughput as more interference is introduced.

This paper characterizes the power interference in CSMA/CA based networks consisting of nodes using directional antenna. The severity of the interference is quantized via an improved form of the *Attacking Case* metric as the original form of this metric was developed for nodes using omnidirectional antenna.

The proposed metric is attractive because it considers nodes using directional or omnidirectional antenna, and it enables the quantization of interference in wireless networks using multiple transmission power schemes. The improved *Attacking Case* metric is useful to study the aggregated throughput of IEEE 802.11 based networks; reducing *Attacking Case* probably results in an increase of aggregated throughput. This reduction can be implemented using strategies such as directional antenna, transmit power control, or both.

1. Introduction

IEEE 802.11 based wireless local area network (WLAN) technologies had a tremendous growth in recent years. Cheap and widely available equipments that can be deployed without a license are some of the factors contributing for the technology to gain popularity. A substantial number of access points (APs) are needed to provide coverage for areas such as a university or a city centre. Further, different entities may setup WLANs in the same geographical area uncoordinated. As a consequence, overlapping WLANs emerge. Lack of planning causes the network to saturate due to interference, and reach its capacity faster. Installing additional APs does not increase the capacity of network beyond a certain limit; moreover, if not done carefully the performance of the network could degrade further due to hidden and exposed nodes.

In wireless networks interference is a fundamental issue. Interference is the disturbance caused by a node's RF transmission into neighboring node(s). High transmission powers increase the number of nodes being interfered. The severity of interference

can be quantized using the performance metric *Attacking Case* [1]. This metric uses information such as nodes position, transmission power, signal to interference ratio and radio propagation model to characterize the instances where simultaneous transmissions are not allowed and, if allowed, the transmission would not be successful. A high *Attacking Case* value indicates a severe interference in the network. Therefore this metric is useful to understand and to optimize the performance of a wireless network.

The IEEE 802.11 standard caters for omnidirectional antenna (OA) [2] but there are many IEEE 802.11 based network deployed using directional antenna (DA) [3–7]. The well known motivations for using DA [8,9] include: (1) a node is able to selectively send signals to desired directions. This allows the receiver node to avoid interference that comes from unwanted directions, thereby increasing the signal to interference and noise ratio (SINR); (2) more users could utilize a network simultaneously due to the spatial reuse factor which is higher than OA; (3) in a multihop network, a source is able to reach its destination node in a lesser number of hops due to the increase of transmission range because of the higher antenna gain. For these reasons, DA may be preferred to OA in some wireless network scenarios.

This paper aims to characterize the power interference for IEEE 802.11 based networks consisting of nodes using DA. To quantize the severity of interference in a wireless network, the *Attacking*

* Corresponding author at: Centre for Telecommunications and Multimedia, INESC TEC, Porto, Portugal. Tel.: +351939786050.

E-mail addresses: kandasamy@inesctec.pt, svanan77@gmail.com (S. Kandasamy), ricardo.morla@inesctec.pt (R. Morla), mricardo@inesctec.pt (M. Ricardo).
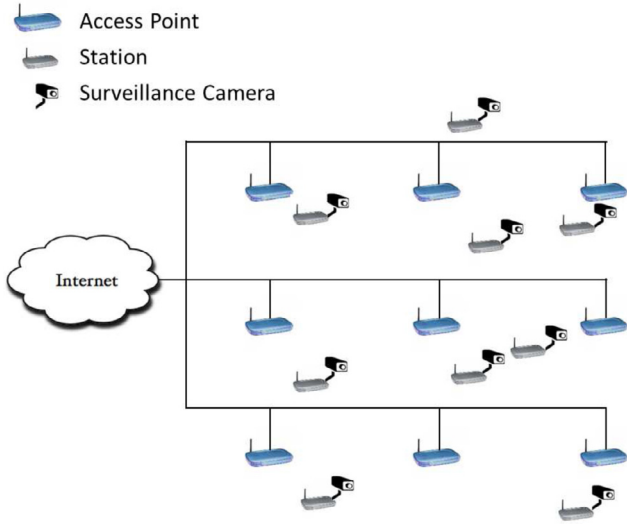
Fig. 1. The wireless videos surveillance network deployed as a basic scenario.

Fig. 2. Taxonomy for interference model.

Case metric defined in [1] is adopted as reference and extended to cater for DA. The Link-Interference Graph, Transmitter-side Protocol Collision Prevention Graph, and Receiver-side Protocol Collision Prevention Graph are used to define the improved *Attacking Case* metric. Power constraints consisting of Physical Collision Constraints and Protocol Collision Prevention Constraints are utilized to model the graphs.

We have considered the wireless video surveillance network shown in Fig. 1 as the basic scenario for our study. A video surveillance camera is attached to an IEEE 802.11 based station (STA) which is randomly placed in a network. The STA will connect to its closest AP placed at a fixed location and send its video traffic towards the AP. In our scenario the APs have access to the Internet via a wired connection. The network operates using the Basic Access Scheme of Distributed Coordinated Function (DCF) of the IEEE 802.11 MAC protocol known as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). When a node (STA or AP) transmits, all other nodes within its power interference range are prohibited from transmitting in the same channel until the end of its current transmission. Individual DATA frames are acknowledged by an ACK frame and retransmission is scheduled by the sender if no ACK is received. Only when the medium is free the other nodes are allowed to transmit after waiting for a random time interval. As each STA is fitted with a video surveillance camera, it always has traffic to send and aggressively competes for accessing the medium.

This paper provides one major contribution – an improved *Attacking Case* metric that quantizes the severity of interference in IEEE 802.11 based networks consisting of nodes using DA. Our current metric differs from Liew's *Attacking Case* metric [1] on the following aspects: (a) the consideration of direction of transmission θ when the power constraints are built; (b) the adoption of Protocol Collision Prevention Constraints using carrier sensing range and transmission range; (c) association of a weight w to the edge of the Link-Interference Graph, Transmitter-side Protocol Collision Prevention Graph, and Receiver-side Protocol Collision Prevention Graph. The improved *Attacking Case* is backward compatible with the former definition and can also be used in networks using OA. Our contribution can be particularly useful for network planners to understand the severity of interference in their network and make remedial actions to reduce it; an interference reduction effort is successful if *Attacking Case*$_{after}$ < *Attacking Case*$_{before}$.
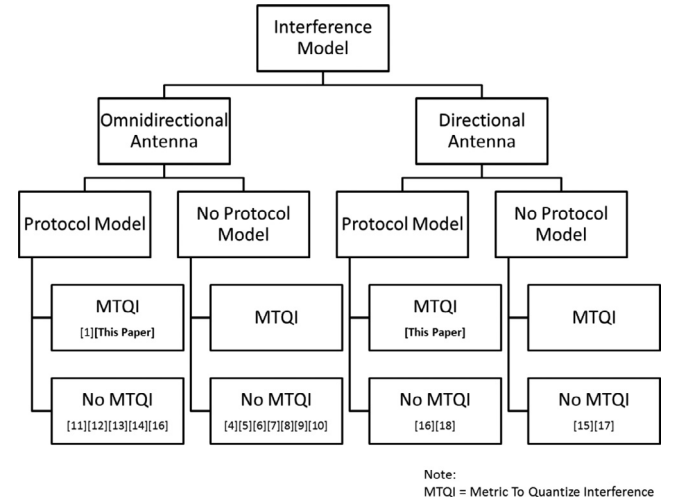
The rest of the paper is organized as follows. In Section 2 we present the related works and show the research space our work fills in. In Section 3 we introduce the power constraints in IEEE 802.11 networks. In Section 4 we present the graph model used to obtain the improved *Attacking Case* metric. The power constraints are utilized to characterize the graph model. In Section 5 we describe the simulation carried out and the performance results obtained. Finally, in Section 6 we draw the conclusions and indicate topics for future work.

2. Related work

In this section we present relevant related works and review the literature from the perspective of interference modeling. Fig. 2 illustrates a possible taxonomy for interference models where the related works are categorized by antenna type, usage of protocol model, and metric to quantize interference. This taxonomy will also be used to describe the research space our work fits in.

The type of antenna a node uses influences the severity of interference in a wireless network. Moraes and Arajo [10] modeled interference for wireless ad hoc network; they found signal to interference plus noise ratio (SINR) approaches a constant value when the number of nodes increases around a receiving node if the path loss parameter is greater than two. Hence, communication is feasible for near neighbors though the number of interferers scales. Liu et al. [11] demonstrated the reduction of interference by tuning the carrier sense threshold; they concluded that the optimum carrier sensing range should be balanced with the spatial reuse and the impact of interference in order to optimize the aggregate throughput of nodes. The works by Renato and Fagner, and Liu et al. including several other recent works in [12–15] have modeled interference for nodes using OA and may not be suitable for nodes using DA. We modeled interference for nodes using DA and our proposed model does also address nodes using OA.

Gupta and Kumar proposed the Protocol Model [16]. Suppose X_i refers to the physical position of node *i*. When node *i* transmits to node *j* using a specific channel, this transmission would be successfully received by node *j*, if

$$|X_k - X_j| \geq (1 + \Delta)|X_i - X_j| \qquad (1)$$

for every node *k* simultaneously transmitting over the same channel. Δ is related to power margin required to ensure the successful reception at node *j* even though node *k* transmits at the same time. The Gupta and Kumar's Protocol Model is said to consider only the DATA to DATA collision constraints between two

simultaneous transmitting links. Ng et al. [17] pointed though Gupta and Kumar's proposed model is named as a Protocol Model it does not fully characterize the medium access protocol being used. Hence, Ho and Liew proposed another model [1] where Physical Collision Constraints and Protocol Collision Prevention Constraints among the DATA and protocol specific control packets were considered. Alawieh et al. [18] have also proposed a model considering the protocol components of a transmission. They studied the relationship between tuning carrier sensing threshold and transmission power control for Basic Access Scheme and RTS/CTS Access Scheme. Although the control packets may slightly reduce the collision among contending hosts, their impact on the spatial reuse and the added overhead outweigh their benefits specifically when used at high rates. This comparative study has showed that the Basic Access Scheme always outperforms the RTS/CTS Access Scheme. Although Liew's and Basel's proposals including the recent works in [19,20] reflect a more accurate model as they have considered a protocol model, they are only suitable for network using OA. We model interference using protocol model for network using DA.

Li et al. [21] have investigated the capacity of wireless networks using DAs. They proposed that the number of beams of DAs need to increase as the number of nodes increases in order for both random and arbitrary networks to scale. Although Li's proposal including the recent works in [22–24] have modeled interference for network using DA they have not proposed a metric to measure the severity of interference. In fact, there are not many works done to quantize the severity of interference in an aggregated form for a wireless network. Parameters such as throughput and packet error ratio do not directly explain the interference in a wireless network. SINR is perhaps the closest way to quantize interference, but it is not a global metric. To the best knowledge of the authors, Ho and Liew [1] is the only work that had quantized the severity of interference and introduced a metric to represent it in a wireless network. Liew proposed the *Attacking Case*, a metric that considers the interference caused by protocol dependent and protocol independent constraints which are captured in graphs. Although very good, the approach was developed for nodes using omnidirectional antenna. We extend the *Attacking Case* metric to cater for nodes using DA.

3. Power constraints in IEEE 802.11 network

A node using DA is able to transmit at one specific angular direction at a time slot and later change direction to transmit at a different angle at another time slot. In this section we extend the Physical Collision Constraints and Protocol Collision Prevention Constraints proposed in [1] to accommodate DA. At the end of the section we discuss the differences between our proposed extensions and Liew's models.

3.1. Physical Collision Constraints

The Physical Collision Constraints can be modeled using the pair-wise interference model. For a link under the pair-wise interference model, the interferences from the other links are considered one by one. In particular, the pair-wise interference model does not take into account the cumulative effects of the interferences from the other links [20].

$$P(a, \theta_b, b) = c(a, \theta_b, b) \cdot P_a^{\theta_b}/r^\alpha \tag{2}$$

where $P(a, \theta_b, b)$ is the power received by node b from the direction θ_b of node a and $P_a^{\theta_b}$ is the power transmitted by node a in the direction of node b as shown in Fig. 3. r is the distance between the two nodes, α is the path-loss exponent, and $c(a, \theta_b, b)$ is a constant in the direction of node b from node a. For instance
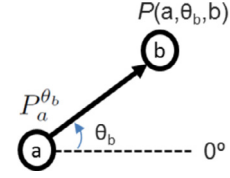

Fig. 3. Transmission power notation for Node a transmitting to Node b.

for two-ray ground reflection radio propagation model α is 4 and $c(a, \theta_b, b)$ is defined as in Eq. 3.

$$c(a, \theta_b, b) = (G_a^{\theta_b} \cdot G_b^{((\theta_b+180°) \bmod 360°)} \cdot h_a^2 \cdot h_b^2) \tag{3}$$

where $G_a^{\theta_b}$ is the gain of node a's antenna in the direction of node b and $G_b^{((\theta_b+180°) \bmod 360°)}$ is gain of node b's antenna in the direction of node a. h_a and h_b are the heights of node a's and node b's antennas respectively. Similar relationship as in Eq. 3 can be derived for other radio propagation models. θ_b in Fig. 3 is suitable to represent any type of directional antenna such as adaptive array antenna, switched beam antenna or several elements of passive directional antennas connected via multiple interfaces. The present definition is straight forward for adaptive array antenna; in switched beam antenna θ_b will translate to the *beam_id* that radiates in the direction of angle θ_b; in multi-interface directional antenna system θ_b will translate to the *interface_id* that radiates in the direction of angle θ_b.

Let us consider two pairs of data links, Link i and Link j, communicating using the Basic Access Scheme of IEEE 802.11 MAC protocol (DATA and ACK) without RTS and CTS. Let T_i and R_i represent respectively the position of the transmitter and receiver of Link i. T_i and R_i are also used for simplicity to refer to the nodes. T_i will transmit DATA and receive ACK while R_i will receive DATA and transmit ACK. Four different possible combination of simultaneous transmissions by Link i and Link j may occur: DATA$_i$-DATA$_j$, DATA$_i$-ACK$_j$, ACK$_i$-DATA$_j$, and ACK$_i$-ACK$_j$. The following Physical Collision Constraints can be derived for the four combinations. For a DATA$_i$-DATA$_j$ pair of transmissions a collision occurs when Link i interferes with Link j. The transmission of Link i will be interfering with the transmission of Link j if,

$$P(T_j, \theta_{R_j}, R_j) < KP(T_i, \theta_{R_j}, R_j) \qquad (\text{DATA}_i\text{-DATA}_j) \tag{4}$$

where K is the Signal to Interference Ratio requirement for a packet to be successfully decoded by the IEEE 802.11 protocol (e.g 10 dB). Independently of T_i transmitting first or T_j transmitting first, as long as the two transmissions overlap in time, T_j's DATA transmission will be interfered at R_j if the constraint in Eq. 4 is satisfied. Similar relationships can be established for the other 3 constraints. The transmission of Link i will interfere with the transmission of Link j if,

$$P(R_j, \theta_{T_j}, T_j) < KP(T_i, \theta_{T_j}, T_j) \qquad (\text{DATA}_i\text{-ACK}_j) \tag{5}$$

$$P(T_j, \theta_{R_j}, R_j) < KP(R_i, \theta_{R_j}, R_j) \qquad (\text{ACK}_i\text{-DATA}_j) \tag{6}$$

$$P(R_j, \theta_{T_j}, T_j) < KP(R_i, \theta_{T_j}, T_j) \qquad (\text{ACK}_i\text{-ACK}_j) \tag{7}$$

3.2. Protocol Collision Prevention Constraints

The Protocol Collision Prevention Constraints of IEEE 802.11 consider the effect of carrier sensing. The goal of carrier sensing is to prevent simultaneous transmissions. The prevention of a transmission can be induced at the transmitter's side, at the receiver's side or at both sides. There are two types of carrier sensing that would prevent a transmission:

Physical Carrier Sensing (PCS) - The PCS defined by IEEE is the clear channel assessment mechanism [2]. When a carrier is sensed

by the radio interface, the clear channel assessment mechanism indicates a busy medium and prevents the radio interface from initiating its own transmission. If a node is within the carrier sensing range (CSRange) of a transmitting node, in presence of no other interference, the PCS mechanism of the node would be triggered every time a packet is detected.

Virtual Carrier Sensing (VCS) - The VCS mechanism is defined in addition to the PCS [2]. VCS uses the information found in IEEE 802.11 packets to predict the status of the wireless medium and determine how long a node has to wait before attempting to transmit. If a node is within the transmission range (TXRange) of a transmitting node, in presence of no other interference, the VCS mechanism of the node would be triggered every time a packet is being detected.

3.2.1. Transmitter side

A transmitter would refrain from transmitting a DATA packet if it can sense the transmission of another ongoing transmission. The transmission of Link i will interfere with the transmission of Link j if,

$$|T_j - T_i| < CSRange\left(P_{T_i}^{\theta_{T_j}}\right) \qquad (DATA_i\text{-}DATA_j) \qquad (8)$$

$$|T_j - R_i| < CSRange\left(P_{R_i}^{\theta_{T_j}}\right) \qquad (ACK_i\text{-}DATA_j) \qquad (9)$$

$$|T_j - T_i| < TXRange\left(P_{T_i}^{\theta_{T_j}}\right) \qquad (DATA_i\text{-}DATA_j) \qquad (10)$$

3.2.2. Receiver side

In IEEE 802.11 commercial products, when T_i is already transmitting, T_j can still transmit if T_i interferes only with R_j but not T_j. However, R_j will ignore the DATA from T_j and not transmit an ACK to T_j fearing it may interfere with the ongoing transmission on Link i [1]. The transmission of Link i will interfere with the transmission of Link j if,

$$|R_j - T_i| < CSRange\left(P_{T_i}^{\theta_{R_j}}\right) \qquad (DATA_i\text{-}ACK_j) \qquad (11)$$

$$|R_j - R_i| < CSRange\left(P_{R_i}^{\theta_{R_j}}\right) \qquad (ACK_i\text{-}ACK_j) \qquad (12)$$

$$|R_j - T_i| < TXRange\left(P_{T_i}^{\theta_{R_j}}\right) \qquad (DATA_i\text{-}ACK_j) \qquad (13)$$

3.3. Power constraints by Liew

Liew, in [1], has modeled the Physical Collision Constraints using Eq. 14. As we are modeling a network with nodes that use DA, Eq. 14 is not suitable for such a network. We have extended Eq. 14 by incorporating the direction of transmission θ as shown in Eq. 2.

$$P(a, b) = c \cdot P_a / r^\alpha \qquad (14)$$

Liew has considered the Virtual Carrier Sensing Range (VCSRange) and the Physical Carrier Sensing Range (PCSRange) when modeling the Protocol Collision Prevention Constraints. VCSRange refers to the virtual carrier sensing ranges by the transmission of RTS/CTS packets and PCSRange refers to the physical carrier sensing ranges by the transmission of DATA packets [1]. For the correct operation of the physical layer we have considered the CSRange and TXRange which is limited by the carrier sensing range and transmission ranges of any packets sent over a wireless channel. This is because non-RTS/CTS packets such as DATA do also have VCS functionally.
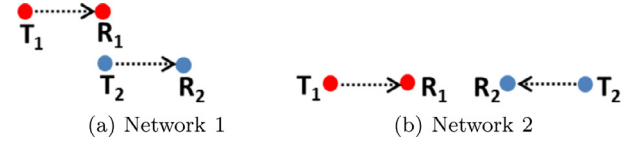

(a) Network 1   (b) Network 2

Fig. 4. Example networks – Networks 1 and 2 – used to capture different interference conditions and to present the 3 graphs.

4. Graph models for attacking case

A graph can be used to represent a network and its relationships. As the Physical Collision Constraints and the Protocol Collision Prevention Constraints are modeled pair-wise, the relationships between objects can easily be represented by means of graphs. In this section these constraints are used to model 3 weighted directed graphs: the Link-Interference Graph, the Transmitter-side Protocol Collision Prevention Graph, and the Receiver-side Protocol Collision Prevention Graph. These graphs will be used to construct our improved *Attacking Case* metric. Let us define the general graph G as a collection of vertices V and unidirectional edges E that connect pairs of vertices with weights w.

$$G = (V, E, w) \qquad (15)$$

For any unidirectional edge $e_{ij} \in E$ where $i, j \in V$, vertex i represents Link i consisting of T_i and R_i nodes, while e_{ij} represents a relationship between Link i and Link j. The weight is a function of e_{ij} where $w(e_{ij}) \in \mathbb{N}$. The value of $w(e_{ij})$ depends on the type graph being modeled.

We introduce the 3 proposed graphs by discussing two simple networks: Networks 1 and 2, shown in Fig. 4. The nodes in the two simple networks are static as our basic scenario is a wireless video surveillance network (Fig. 1) consisting of nodes that are not mobile. For the sake of analysis simplicity: (a) the distances of transmitter-receiver pairs, R_1 and T_2 in Network 1, and R_1 and R_2 in Network 2 are set to 200 m; (b) the ranges are defined based on a two-ray ground reflection radio propagation model; (c) the effect of cross over distance together with the random component for shadowing are not considered; (d) K is set to 10 dB. Each network is analyzed for 3 different setups where a setup is characterized by the type of antenna used (omnidirectional, directional) and by the ranges of a node (TXRange, CSRange).

The 3 setups addressed are the following:

(a) Omnidirectional Antenna Setup (OA Setup) - Antenna = Omnidirectional, Gain = 1, Node's transmission power P_{OA} = 282 mW, TXRange = 250 m, CSRange = 550 m;
(b) Directional Antenna Setup (DA Setup) - Antenna = Directional ($90°$ beamwidth), Gain = 2, Node's transmission power $P_{DA} = P_{OA}$, TXRange = 374 m, CSRange = 778 m;
(c) Directional Antenna with Reduced Transmit Power Setup (DR Setup) - Antenna = Directional ($90°$ beamwidth), Gain = 2, Node's transmission power such that *transmit range* (P_{DR}) = *transmit range* (P_{OA}), TXRange = 250 m, CSRange = 550 m.

Fig. 5 describes the 2 networks and the 3 setups along with their TXRanges and CSRanges.

4.1. Link-Interference Graph (i-graph)

A Link-Interference Graph is used to represent the Physical Collision Constraints and it captures the Signal to Interference Ratio effects among links. The graph is represented as follows:

$$G_I = (V_I, E_I, w_I) \qquad (16)$$

(a) Network 1 - OA Setup

(b) Network 2 - OA Setup

(c) Network 1 - DA Setup

(d) Network 2 - DA Setup
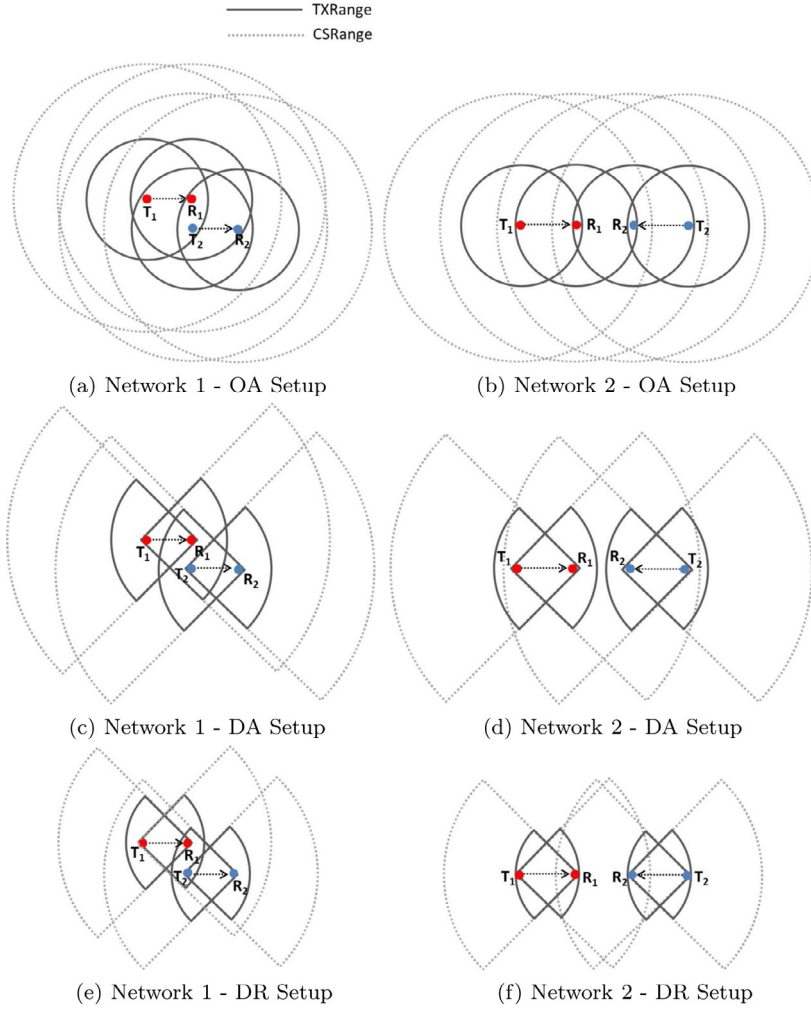
(e) Network 1 - DR Setup

(f) Network 2 - DR Setup

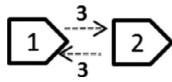Fig. 5. TXRanges and CSRanges representation for 3 setups for Networks 1 and 2.

Fig. 6. i-graph for the network in Fig. 5a.

The i-graph of the network topology illustrated in Fig. 5a can be represented by the graph in Fig. 6. In the figure, an arrow-shaped vertex represents a wireless link with the arrow pointing towards the receiver of the link. Each vertex is labeled with the *link_id* (Link 1 or Link 2) it represents. An arrow connects vertex 1 to vertex 2 if there is a relationship from Link 1 to Link 2. The edge e_{ij} is labeled with its $w_I(e_{ij})$.

Consider the topology of Fig. 5a where the nodes use OA. There is a directional i-edge, shown in Fig. 6, from vertex 2 to vertex 1 because the transmitter of Link 2 interferes with receiver of Link 1. More specifically, DATA transmitted by T_2 will collide with a DATA transmitted by T_1 at R_1 if the transmissions overlap in time since, in this case, Eq. 4 holds (DATA$_2$-DATA$_1$). In the reverse direction, there is no i-edge from vertex 1 to vertex 2 due to DATA$_1$-DATA$_2$ pair of transmission but there is an i-edge from vertex 1 to vertex 2 due to DATA$_1$-ACK$_2$, ACK$_1$-DATA$_2$, and ACK$_1$-ACK$_2$ pairs of transmission. There are also i-edges from vertex 2 to vertex 1 due to DATA$_2$-ACK$_1$ and ACK$_2$-DATA$_1$ pairs of transmissions.

In general, if any of the constraints in Eq. 4, 5, 6 or 7 is satisfied, an edge would be drawn from vertex i to vertex j to signify that Link i is interfering with Link j. We propose that the unidirectional edge in the i-graph has a weight $w_I(e_{ij})$ characterized as follows:

$$
w_I(e_{ij}) = \mathbb{1}_{\left[P_{T_j}^{\theta_{R_j}} |T_i - R_j|^\alpha < K P_{T_i}^{\theta_{R_j}} |T_j - R_j|^\alpha \right]} + \\
\mathbb{1}_{\left[P_{R_j}^{\theta_{T_j}} |T_i - T_j|^\alpha < K P_{T_i}^{\theta_{T_j}} |T_j - R_j|^\alpha \right]} + \\
\mathbb{1}_{\left[P_{T_j}^{\theta_{R_j}} |R_i - R_j|^\alpha < K P_{R_i}^{\theta_{R_j}} |T_j - R_j|^\alpha \right]} + \\
\mathbb{1}_{\left[P_{R_j}^{\theta_{T_j}} |R_i - T_j|^\alpha < K P_{R_i}^{\theta_{T_j}} |T_j - R_j|^\alpha \right]}
$$

(17)

where Eq. 17 is built using components of characteristic function as defined in Eq. 18.

$$
\mathbb{1}_{[C]} = \begin{cases} 1, & if\ C = TRUE \\ 0, & if\ C = FALSE \end{cases}
$$

(18)

Since $w_I(e_{ij})$ exists only when there is an e_{ij}, $w_I(e_{ij}) \in \{1, 2, 3, 4\}$ for i-graph. For the OA setup in Fig. 5a, its i-graph has directional edge from vertex 1 and vertex 2 and vice versa with weight $w_I(e_{12}) = w_I(e_{21}) = 3$.

In Fig. 5c the antenna is directional. Although i-edges exist as in OA setup from vertex 1 to vertex 2 due to DATA$_1$-ACK$_2$ pair of
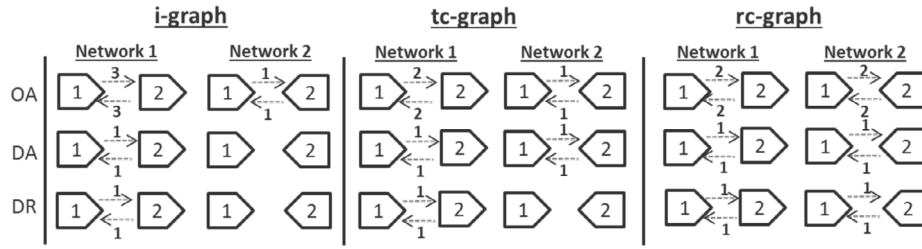
Fig. 7. Graph Models of the networks and setups presented in Fig. 5 using our proposed method.

transmissions and vice versa, the i-edges due to the other transmission pairs do not exist. The ability of DA to point its beam to its intended destination reduces interference on unwanted directions. For the setup in Fig. 5c, $w_I(e_{12}) = w_I(e_{21}) = 1$ and the i-graph obtained can be observed in Fig. 7.

In Fig. 5e the i-graph obtained is the same as in DA setup, where i-edges exist from vertex 1 to vertex 2 due to DATA$_1$-ACK$_2$ pair of transmissions and vice versa. The reduction of transmission power has no gain for i-graph in this topology. For the setup in Fig. 5e, $w_I(e_{12}) = w_I(e_{21}) = 1$ and Fig. 7 shows the i-graph obtained.

In Fig. 5b a different node positioning is tested and the nodes use OA. In the figure we can observe that there are directional i-edges from vertex 1 to vertex 2 due to ACK$_1$-DATA$_2$ pair of transmission and from vertex 2 to vertex 1 due to ACK$_2$-DATA$_1$ pair of transmission. $w_I(e_{12}) = w_I(e_{21}) = 1$ for the i-graph and this is shown in Fig. 7. We recall that in Fig. 5a the weight was 3, hence the topology of a network affects the outcome of an i-graph and its edge's weight.

In Fig. 5d and Fig. 5f no pair of transmission creates an i-edge between vertex 1 and vertex 2, and vice versa; in these setups the antenna type plays an important role in eliminating edges between the vertices.

From Figs. 5 and 7 we can conclude that the DA and DR setups lead to the smallest interference. The OA setup has the highest value of weight on the i-edges. The more weight an i-edge has the more prone it gets for packet collision. Network 1 and Network 2 enable us to conclude that the topology affects the weight of an i-edge.

4.2. Transmitter-side Protocol Collision Prevention Graph (tc-graph)

Let us consider the effect of IEEE 802.11 carrier sensing. The goal of carrier sensing is to prevent simultaneous transmissions that will collide. The tc-graph models the effect of carrier sensing by the transmitters and it is represented as follows:

$$G_{TC} = (V_{TC}, E_{TC}, w_{TC}) \qquad (19)$$

In the tc-graph there is a directional tc-edge from vertex i to vertex j if T_j can sense the transmission on Link i so that, if T_i or R_i are already transmitting respectively a DATA or ACK packet, T_j will not transmit. Formally, there is a tc-edge from vertex i to vertex j if any of the Eq. 8, 9 or 10 holds true.

In Fig. 5a, T_1 and T_2 are not sufficiently far apart and they can sense each other. There is directional tc-edge from vertex 1 to vertex 2 because the transmitter of Link 1 interferes with the transmitter of Link 2. Specifically, the transmission of DATA from T_1 and ACK from R_1 will prevent DATA from T_2 to be transmitted. There is also a directional tc-edge in the reverse direction; the transmission of DATA from T_2 and ACK from R_2 will prevent DATA from T_1 for being transmitted.

The edge in the tc-graph has a weight $w_{TC}(e_{ij})$ characterized as follows:

$$w_{TC}(e_{ij}) = \mathbb{1}_{\left[\left(|T_j - T_i| < CSRange\left(P_{T_i}^{\theta_{T_j}}\right)\right) \vee \left(|T_j - T_i| < TXRange\left(P_{T_i}^{\theta_{T_j}}\right)\right)\right]}^{+} \\ \mathbb{1}_{\left[|T_j - R_i| < CSRange\left(P_{R_i}^{\theta_{T_j}}\right)\right]} \qquad (20)$$

Since $w_{TC}(e_{ij})$ exists only when there is an e_{ij}, $w_{TC}(e_{ij}) \in \{1, 2\}$ for tc-graph. For the setup in Fig. 5a, $w_{TC}(e_{12}) = w_{TC}(e_{21}) = 2$ and the tc-graph obtained can be observed in Fig. 7.

As the tc-graph models the effect of carrier sensing purely from the transmitter point of view, it does not consider tc-edges created due to the DATA$_1$-ACK$_2$ and ACK$_1$-ACK$_2$ pairs of transmission from vertex 1 to vertex 2 and DATA$_2$-ACK$_1$ and ACK$_2$-ACK$_1$ pairs of transmission from vertex 2 to vertex 1 due to its effect solely at the receiver.

In Fig. 5c the antenna is directional. There are tc-edges from vertex 1 to vertex 2 due to DATA$_1$-DATA$_2$ pair of transmission and from vertex 2 to vertex 1 due to ACK$_2$-DATA$_1$ pair of transmission. The tc-edges which occur in OA setup for ACK$_1$-DATA$_2$ and DATA$_2$-DATA$_1$ do not exist in DA setup. This is because of the ability of DA to point its beam to its intended receiver which also reduces interference to unwanted directions. For the setup in Fig. 5c, $w_{TC}(e_{12}) = w_{TC}(e_{21}) = 1$ and its tc-graph is shown in Fig. 7.

In Fig. 5e the tc-graph is the same as for the DA setup, where tc-edges exist from vertex 1 to vertex 2 due to DATA$_1$-DATA$_2$ and from vertex 2 to vertex 1 due to ACK$_2$-DATA$_1$ pairs of transmission. As in i-graph, the transmission power reduction has no gain for tc-graph for this topology. $w_{TC}(e_{12}) = w_{TC}(e_{21}) = 1$ for the scheme in Figs. 5e, and 7 shows the tc-graph observed.

For Network 2 using OA (Fig. 5b) there are directional tc-edges from vertex 1 to vertex 2 due to ACK$_1$-DATA$_2$ pair of transmission and from vertex 2 to vertex 1 due to ACK$_2$-DATA$_1$ pair of transmission. The weight, $w_{TC}(e_{12}) = w_{TC}(e_{21}) = 1$. We recall that in Fig. 5a the weight was 3 and reaffirm that network topology affects the outcome of an tc-graph and its edge's weight.

In Fig. 5d the antenna is directional. The ACK$_1$-DATA$_2$ and ACK$_2$-DATA$_1$ pairs of transmission which were present in the OA setup do not cause tc-edges anymore, but the DATA$_1$-DATA$_2$ and vice versa pairs of transmission cause tc-edges for the DA setup. This is because though interference is able to be contained on unwanted direction, it actually increased in the direction of transmission when DA is used. For the setup in Fig. 5d, $w_{TC}(e_{12}) = w_{TC}(e_{21}) = 1$ and its resultant tc-graph is shown in Fig. 7.

In Fig. 5f none of the pairs of transmission create a tc-edge between vertex 1 and vertex 2 and vice versa. In this case, DA and transmission power reduction have played an important role in eliminating edges between the vertices.

From Figs. 5 and 7 we can conclude that the DA and DR setups lead to the smallest interference. The more weight a tc-edge has the more a node will trigger its exponential backoff mechanism.

Networks 1 and 2 enable us to conclude that, as in i-graph, the topology affects the weight of tc-edges.

4.3. Receiver-side Protocol Collision Prevention Graph (rc-graph)

In rc-graph the effect of carrier sensing by receivers is modeled. The graph is represented as follows:

$$G_{RC} = (V_{RC}, E_{RC}, w_{RC}) \qquad (21)$$

There is a directional rc-edge from vertex i to vertex j if R_j can sense the transmission on Link i. Specifically, there is an rc-edge from vertex i to vertex j if any of Eq. 11, 12 or 13 is true. In the default mode of IEEE 802.11 commercial products, when T_i is already transmitting, T_j can still transmit if there is an rc-edge, but no tc-edge, from vertex i to vertex j. However, R_j will ignore the DATA frame and will not return an ACK [1]. The rationale for R_j not returning an ACK to T_j is that the ACK may interfere with the ongoing transmission on Link i.

In Fig. 5a, R_1 and R_2 are so close to each other that the DATA and ACK transmission of Link 1 can be sensed by R_2 and the DATA and ACK transmission of Link 2 can be sensed by R_1. Thus, there is a directional rc-edge from vertex 1 to vertex 2 and vice versa.

An edge in the rc-graph has a weight $w_{RC}(e_{ij})$ characterized as follows:

$$w_{RC}(e_{ij}) = \mathbb{1}_{\left[\left(|R_j - T_i| < CSRange\left(P_{T_i}^{\theta_{R_j}}\right)\right) \vee \left(|R_j - T_i| < TXRange\left(P_{T_i}^{\theta_{R_j}}\right)\right)\right]} + $$
$$\mathbb{1}_{\left[|R_j - R_i| < CSRange\left(P_{R_i}^{\theta_{R_j}}\right)\right]} \qquad (22)$$

Since $w_{RC}(e_{ij})$ exist only when there is an e_{ij}, $w_{RC}(e_{ij}) \in \{1, 2\}$ for rc-graph. For the case of Fig. 5a, $w_{RC}(e_{12}) = w_{RC}(e_{21}) = 2$ and its rc-graph is shown in Fig. 7.

Since rc-graph models the effect of carrier sensing purely from the receiver point of view, it does not consider rc-edges created due to the ACK$_1$-DATA$_2$ and DATA$_1$-DATA$_2$ pairs of transmission from vertex 1 to vertex 2, and ACK$_2$-DATA$_1$ and DATA$_2$-DATA$_1$ pairs of transmission from vertex 2 to vertex 1.

In Fig. 5c and in Fig. 5e rc-edges were created in both the setups due to DATA$_1$-ACK$_2$ pair of transmission from vertex 1 to vertex 2 and ACK$_2$-ACK$_1$ pair of transmission from vertex 2 to vertex 1. For the cases of Figs. 5c and 5e, $w_{RC}(e_{12}) = w_{RC}(e_{21}) = 1$ and its rc-graphs are shown in Fig. 7. DA has contributed to reduce the weight of the edges.

In Fig. 5b there is rc-edge from vertex 1 to vertex 2 due to DATA$_1$-ACK$_2$ and ACK$_1$-ACK$_2$ pairs of transmission. There is also rc-edge from vertex 2 to vertex 1 due to DATA$_2$-ACK$_1$ and ACK$_2$-ACK$_1$ pairs of transmission. For the setup in Fig. 5b, $w_{RC}(e_{12}) = w_{RC}(e_{21}) = 2$ and its resultant rc-graph is shown in Fig. 7.

In Figs. 5d and 5f both the setups have rc-edges due to DATA$_1$-ACK$_2$ pair of transmission from vertex 1 to vertex 2 and DATA$_2$-ACK$_1$ pair of transmission from vertex 2 to vertex 1. The weight $w_{RC}(e_{12}) = w_{RC}(e_{21}) = 1$.

From Figs. 5 and 7 we can conclude that the DA and DR setups are able to contain interference and assist in reducing the weight of the edges. The transmission power control has no advantage for these networks as the power reduced is still insufficient to curtail interference in the direction of DA's transmission.

For i-graph, tc-graph and rc-graph all the vertices are the same, where $V = V_I = V_{TC} = V_{RC}$.

4.4. Improved Attacking Case Metric

Attacking Case corresponds to the number of cases where simultaneous transmissions are either not allowed or if allowed will not be successful and this is characterized by the tc-graph, rc-graph and i-graph. *Attacking Case* can be used as a performance metric to quantize the interference of a network. A high *Attacking Case* value leads to potentially poor aggregated network throughputs. We propose the following: (1) if $e_{i,j}$ is an i-edge then twice the i-edge's weight is added to the *Attacking Case* else; (2) if $e_{i,j}$ is a tc-edge then the tc-edge's weight is added to the *Attacking Case*, and (3) if $e_{i,j}$ is a rc-edge then the rc-edge's weight is added to the *Attacking Case* for all i, j where $i \neq j$ as shown in Eq. 23.

$$AC_{Imp} = \sum_{\substack{i,j \in V \\ i \neq j}} \Big[2 \times w_I(e_{i,j}) \times \mathbb{1}_{[e_{i,j} \in E_I]} + $$
$$w_{TC}(e_{i,j}) \times \mathbb{1}_{[e_{i,j} \in E_{TC} \wedge e_{i,j} \notin E_I]} + $$
$$w_{RC}(e_{i,j}) \times \mathbb{1}_{[e_{i,j} \in E_{RC} \wedge e_{i,j} \notin E_I]} \Big] \qquad (23)$$

Eq. 23 takes into account the order of transmissions. If $e_{i,j}$ is an i-edge, it does not matter whether Link i or Link j transmits first, the packet at Link j will be corrupted. Hence, there are two cases where Link i can interference with Link j. For this reason twice the weight of i-edges are added to the *Attacking Case* if the edges are present. On the other hand if $e_{i,j}$ is a tc-edge or rc-edge, transmission at Link j will not be allowed or will fail only if Link i transmits first. So, there is only one case considered and the respective weight of tc-edges or rc-edges are added to the *Attacking Case* if the edges are present.

4.5. Graph Models for Liew's Attacking Case

Liew in [1] has modeled the *Attacking Case* using the graph model in Eq. 24.

$$G = (V, E) \qquad (24)$$

We have extended Eq. 24 by associating it with weights w to the edge of the Link-Interference Graph, Transmitter-side Protocol Collision Prevention Graph, and Receiver-side Protocol Collision Prevention Graph as shown in Eq. 15.

In Liew's method, if $e_{i,j}$ is an i-edge then 2 is added to the *Attacking Case*, else if $e_{i,j}$ is a tc-edge then 1 is added to the *Attacking Case*, else if $e_{i,j}$ is a rc-edge then 1 is added to the *Attacking Case* for all i, j where $i \neq j$, as shown in Eq. 25. We have improved Liew's method by considering the weights of the graphs and the method used to calculate the *Attacking Case* metric using the i-graph, tc-graph and rc-graph, as shown in Eq. 23.

$$AC_{Liew} = \sum_{\substack{i,j \in V \\ i \neq j}} \Big[2 \times \mathbb{1}_{[e_{i,j} \in E_I]} + $$
$$\mathbb{1}_{[e_{i,j} \in E_{TC} \wedge e_{i,j} \notin E_I]} + $$
$$\mathbb{1}_{[e_{i,j} \in E_{RC} \wedge e_{i,j} \notin E_{TC} \wedge e_{i,j} \notin E_I]} \Big] \qquad (25)$$

5. Attacking Case Metric Evaluation

In this section the improved *Attacking Case* metric (Eq. 23) is used to quantize the severity of interference in CSMA/CA based networks by means of Network Simulator 2 (ns-2) simulations [25]. Firstly we show that the Liew's *Attacking Case* metric does not address nodes using DA. Secondly we show that our improved *Attacking Case* supports nodes using DA and it is also compatible for nodes using OA. Thirdly we show that our improved *Attacking Case* metric is able to quantize the interference for networks that use various transmission power schemes.

5.1. ns-2 simulator enhancements

When a node hears the arrival of packet A via clear channel assessment mechanism, the packet is received by the node if the received power is above a certain threshold. First, the node's physical layer decodes the packet's Physical Layer Convergence Protocol
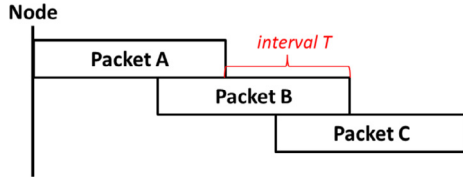
Node

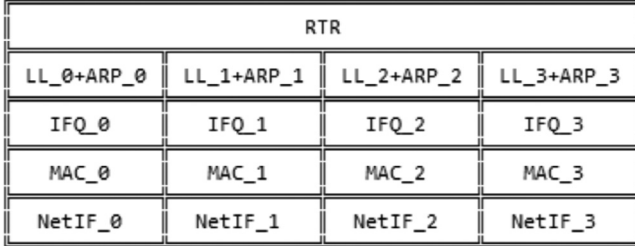**Fig. 8.** Time interval T when packets A, B and C arrive at a Node.

Fig. 9. Directional antenna stack for a wireless node in ns-2.
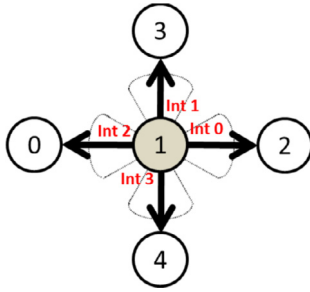

Fig. 10. Directional antenna model for a wireless node in ns-2.

(PLCP) Preamble and PLCP Header. In this process, the node will learn the characteristics of the forthcoming PLCP Service Data Unit (PSDU) such as the modulation used and length of the forthcoming PSDU segment in microseconds. Then the PHY-RXSTART primitive will be initiated if the cyclic redundancy check of the PLCP header is positive. The length field of the PLCP header will determine the end of sending the PSDU octets to the MAC layer. This is done via the PHY-RXEND primitive. During the process of receiving packet A, if another packet B reaches this node overlapping in time and if its power is high enough, then the bits received from packet A are corrupted. The cyclic redundancy check of packet A's PSDU will fail at the end of PHY-RXEND at the MAC layer. If any other packet, say packet C, reaches this node during the time interval *T* of Fig. 8, packet C may be received provided its received power is above the predefined Signal to Interference Ratio. The current behavior of ns-2 does not consider this aspect and disregards packet C [25]. We have extended the ns-2 simulator to consider this as we are studying scenarios operating in the overloaded conditions.

ns-2 was also improved to support nodes with DA. Each node is assumed to have 4 interfaces where each interface is connected to a 90° passive DA. The DA consists in an ideal pie-slice radiation pattern of gain 2 without side or back lobes. The stack to support DA on a node is shown in Fig. 9 where each interface has a MAC, NAV, its own interface queue, and maintains its own address resolution protocol table. The DA in interfaces 0, 1, 2 and 3 are pointed respectively to angle 0°, 90°, 180°, and 270°. As an example please refer to Node 1 in Fig. 10. Node 1 reaches: Node 2 via Interface 0 pointed at 0° angle; Node 3 via Interface 1 pointed at 90° angle; Node 0 via Interface 2 pointed at 180° angle; Node 4 via Interface 3 pointed at 270° angle.

Table 1
Parameter settings used in ns-2.33 simulations.

Parameter	Setting
Access Scheme	Basic Access Scheme (DATA, ACK)
Rate	11 Mbit/s (Data), 1 Mbit/s (Basic)
MAC	IEEE 802.11b
Offered Load	55 packet/s/node
Traffic Packet Size	1500 bytes
Interface Queue Length	50 packets
Signal to Interference Ratio	10 dB
Propagation	Two Ray Ground Reflection
Contention Window	31 (Min), 1023 (Max)
ns-2's Default Transmit Power	281.84 mW
Threshold	RX:3.65e-10 W, CS:1.79e-12 W
Traffic	UDP, Poisson process, 1818.181μs mean inter-arrival interval
Simulation Time	120 s
Type of Antenna	OA, DA
Antenna Gain	OA:1, DA:2
Number of DA/node	4, 90° beamwidth each
Directional Antenna Angles	0°, 90°, 180°, 270°
Node Mobility	Static
Number of Simulations for Each Scenario	40
Number of STAs	9, 18, 27, 36

5.2. Simulation setup

We defined a 3 x 3 grid topology with nodes separated by 250 m and acting as APs. Additional nodes were placed randomly to represent STAs, where each STA will connect to the AP with the strongest signal which is naturally the closest AP. Traffic is sent from the STAs towards the APs replicating the video surveillance network scenario of Fig. 1. Being a single hop wireless network, routing was not considered. All the nodes are static. The number of random STAs in the network varied from 9 to 18, 27, and 36, aiming to increase the amount of interference in the network. For each scenario, 40 random topologies were simulated. As we aim to study high interference, the network operates in single channel to induce high interference in the network. In actual wireless networks which normally operate using multi-channel, high interferences only occur in each channel when the number of STAs increase in greater number than 36 used for our setup. The other parameters used in the simulation are shown in Table 1. The traffic load is chosen such that the interface queue always have a packet to send. Some examples of the random topologies used in the simulation are shown in Fig. 11 when OA are used and the number of STA is 9; the solid lines represent data links, the dashed lines represent nodes within receiving range, and the dotted lines represent nodes within carrier sensing range. As a node with directional antenna uses 4 interfaces, for correct comparison of aggregated throughput for a network using OA each node is fitted with 4 interfaces of OA. In practice only one interface will be active at any one time due to carrier sensing among interfaces.

5.3. Attacking Case

We evaluate our improved *Attacking Case* metric against Liew's *Attacking Case* over a wireless network and compare the results of both. The value of *Attacking Case* indicates the potential for packet collisions and exponential backoffs in a wireless network; the higher the value of *Attacking Case* the smaller will be the aggregated throughput observed in the network.

Using the setup described in Section 5.2, the simulation results for *Attacking Case* for networks with nodes using OA and DA are presented in Figs. 12 and 13. The solid lines represent networks with nodes using OA and the dashed lines represent networks with nodes using DA. The x-axis captures the total number of STAs in
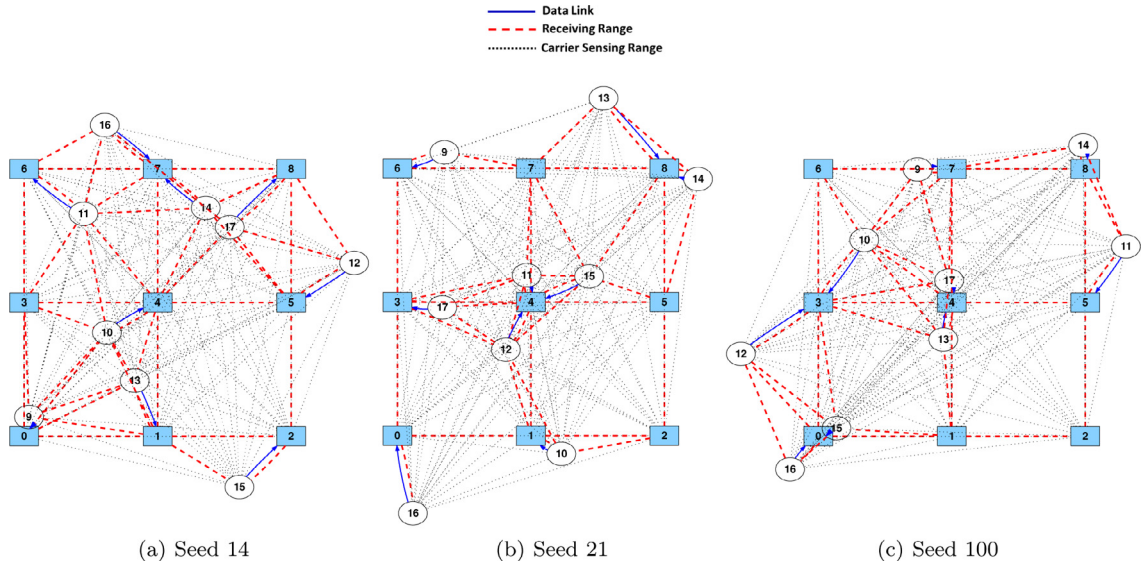
(a) Seed 14   (b) Seed 21   (c) Seed 100

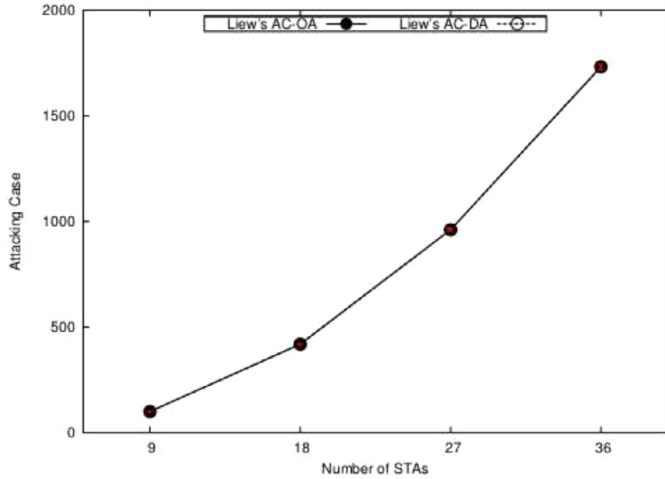**Fig. 11.** Example of random topologies for network with nodes using OA and 9 STAs.

Fig. 12. Liew's *Attacking Case* metric for OA and DA when the number of STAs increase. OA line overlaps with DA line for all the number of STAs.
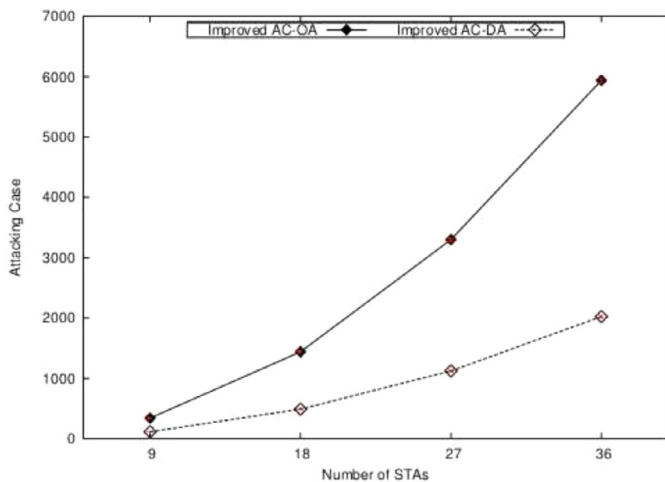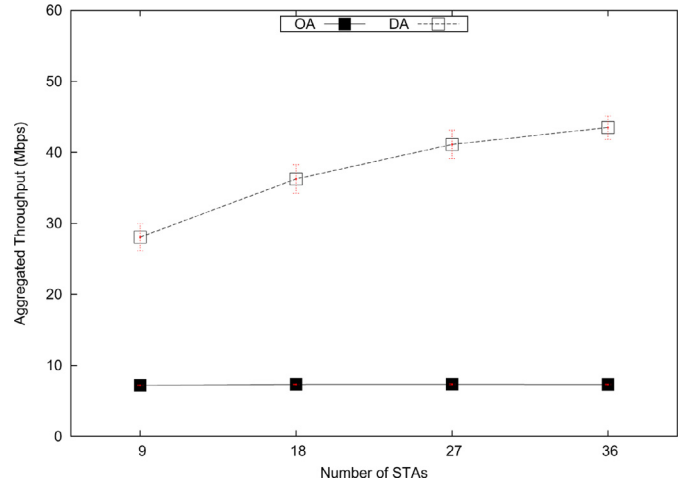

Fig. 14. The aggregated network throughput for OA and DA when the number of STAs increase. Throughput increases when interference is reduced e.g when nodes using DA as captured by the improved *Attacking Case* in Fig. 13.

Fig. 13. The improved *Attacking Case* metric for OA and DA when the number of STAs increase.

the network. The number of STAs were increased by incrementing the STA/AP ratio (1, 2, 3, 4). On the y-axis, the *Attacking Case* in the network is calculated using Liew's approach in Fig. 12 and our improved approach in Fig. 13. The simulation results for aggregated network throughput are also presented in Fig. 14 against the total number of STAs in the network. Fig. 12 illustrates Liew's *Attacking Case* and Fig. 13 illustrates the improved *Attacking Case*. Both figures have two curves each, representing respectively the OA and DA cases. In Fig. 14, there are two curves for the aggregated throughput for network using nodes with OA and DA.

5.3.1. Liew's Attacking Case and Directional Antenna

Firstly, we show that the Liew's *Attacking Case* does not model adequately networks consisting of nodes using DA. In Fig. 12 Liew's *Attacking Case* is presented by the lines with circle points. We can observe that the value of Liew's *Attacking Case* increases as the number of STAs increase due to the surge of interference. However the OA line overlaps with the DA line though the interference is reduced due to the capability of DA to reduce interference on unwanted directions. There are two reasons for this: (a) weight of edges $w(e_{ij})$ – the Liew's *Attacking Case* metric is calculated using

Fig. 15. I-graph using Liew's method for Network 2 with nodes using DA.

Eq. 25. As the edge's weight is not considered in its calculation and only depends on the presence of an edge, the *Attacking Case* value for OA and DA is the same using Liew's approach. For Network 1 in Fig. 7, the *Attacking Case* calculated using Liew's method is 8 for both OA and DA; (b) direction of transmission, θ – the *Attacking Case* calculated using Liew's method for Network 2 in Fig. 7 is 8 for OA; this value considers the i-edges caused by ACK_2-$DATA_1$ and ACK_1-$DATA_2$ pairs of transmissions. For DA though the i-edges due to ACK_2-$DATA_1$ and ACK_1-$DATA_2$ are no longer present because the DA is able to point its beam to its intended direction and reduce interference on unwanted direction, but since θ was not considered by Liew for the construction of the power constraints the same i-graph would result for DA and OA. The resultant i-graph for Network 2 using Liew's method is shown in Fig. 15. Thus the *Attacking Case* value for DA will be the same as OA. In conclusion, the *Attacking Case* metric calculated by Liew gives the same value for OA and DA irrespective of the number of STAs, as shown in Fig. 12. However when the aggregated network throughput of OA and DA is evaluated in Fig. 14 there are big differences between them. DA's throughput outperforms OA by at least 290% for the case of 9 STAs, calculated according to Eq. 26. This suggests Liew's *Attacking Case* is not adequate to quantize the severity of interference for networks with nodes using DA.

$$Gain = (Tput_{DA} - Tput_{OA}) \times 100/Tput_{OA} \tag{26}$$

5.3.2. Improved Attacking Case supporting Directional Antenna

Secondly we show that our improved *Attacking Case* supports nodes using DA and it is also compatible with nodes using OA. In Fig. 13 the improved *Attacking Case* is presented by the lines with diamond shaped points. It can be observed that the value of *Attacking Case* increases as the number of STAs increase for both OA and DA. The OA increases with higher slopes than DA. It can also be seen that the improved *Attacking Case* no longer causes overlapping lines between OA and DA. This is because the weight of edges $w(e_{ij})$ and direction of transmission θ considered in our method are important parameters to characterize the interference caused by nodes using DA. When the number of STAs is 36, the improved *Attacking Case* for OA is approximately 5220 and when the DA setup is used the value decreases to 1840, showing the potential high gain foreseeable in throughput. This is confirmed by the throughput lines in Fig. 14 where DA performed close to 500% better than the OA for the case of 36 STAs. This shows that our improved *Attacking Case* is able to model nodes using DA or OA.

In Fig. 14, as the number of STAs increase the aggregated throughput for DA increases but the rate of increase reduces. This is because the network with nodes using DA is getting saturated. Adding more STAs though increase the amount of offered load to the network unfortunately the network unable to transport more packets due to high exponential backoffs and collisions persist in the network. For OA, due to the nature of the antenna transmitting at all direction, the network gets saturated at much lower STAs than DA as shown in Fig. 14. Due to this reason the aggregated throughput is constant for OA even though the *Attacking Case* in Fig. 13 increases.

5.3.3. Using improved Attacking Case in networks with various transmission power

Thirdly, we show that the improved *Attacking Case* metric is useful to quantize the severity of interference in networks where various transmission powers are used. Let us define the default
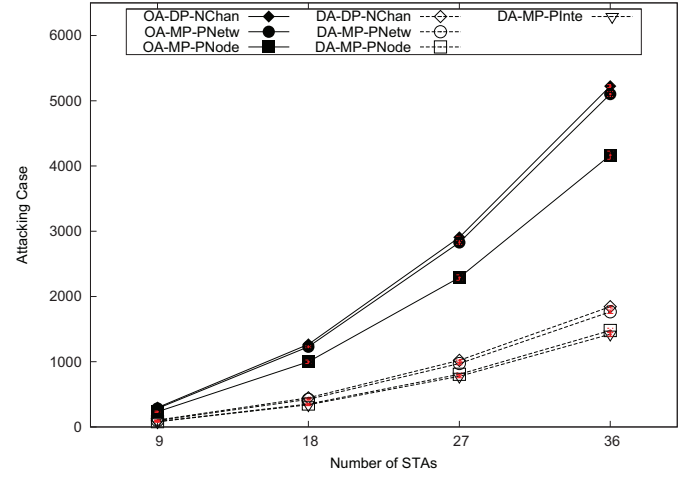

Fig. 16. The improved *Attacking Case* metric for OA and DA for various transmission power strategies when the number of STAs increase.
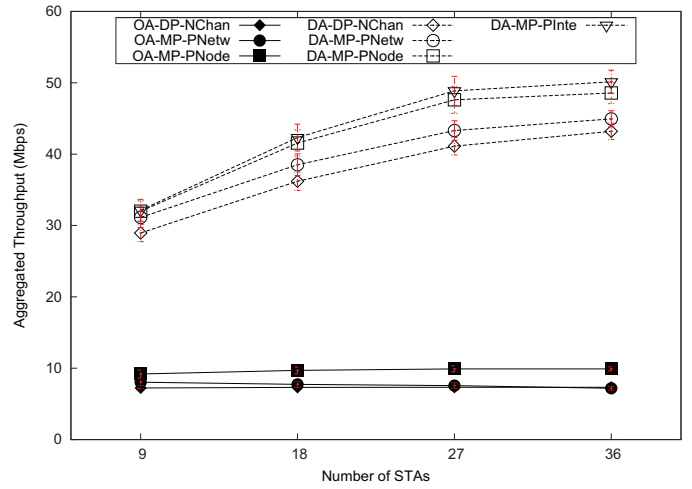

Fig. 17. The aggregated network throughput for OA and DA for various transmission power strategies when the number of STAs increase.

transmission power in ns-2 as DP-NChan [25]. In order to evaluate different levels of interference and its effect on *Attacking Case*, apart from using DP-NChan, the network is also simulated using a minimum transmit power (MP) approach. In this approach the transmission power is enough for a transmitter node to get its transmitted packets decoded by its receiving node. We studied the minimum transmit power approach by using the following 3 setups:

- The minimum power per network (MP-PNetw) – in this setup the interfaces in nodes are allowed to reduce its transmission power, but all the interfaces in the network must use the same transmission power. OA and DA use it.
- The minimum power per node (MP-PNode) – in this setup, as above, the interfaces are allowed to reduce its transmission power. Each node is allowed to have its own transmission power but all the interfaces of a node must use the same power. OA and DA use it.
- The minimum power per interface (MP-PInte) – in this setup each interface is allowed to reduce and use its own transmission power. Only DA uses this.

The rest of the parameters used for the simulations are shown in Table 1. The simulation results are shown in Figs. 16–18.

Table 2
The components of Eq. 25 and the resultant *Attacking Case* using Liew's method when the number of STAs is 36.

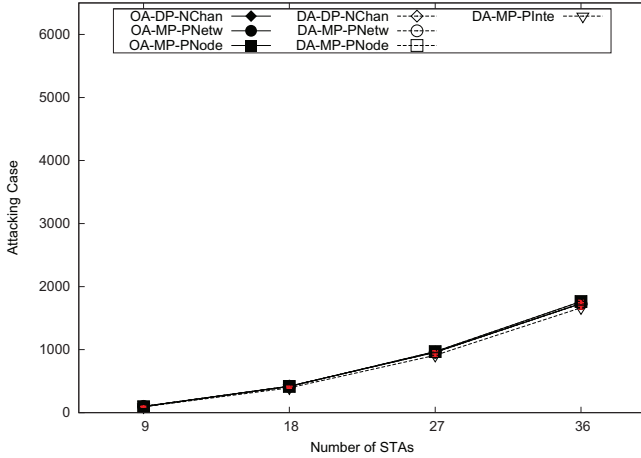| Method	Setup	Component 1 (Eq. 27)	Component 2 (Eq. 28)	Component 3 (Eq. 29)	AC_{Liew}
OA	DP-Nchan	472.1	787.9	0.0	1732.1
	MP-PNetw	472.1	763.8	21.8	1729.8
	MP-PNode	549.1	614.7	51.3	1764.1
DA	DP-Nchan	472.1	787.9	0.0	1732.1
	MP-PNetw	472.1	763.8	21.8	1729.8
	MP-PNode	549.1	614.7	51.3	1764.1
	MP-Pinte	518.1	564.0	64.6	1664.7

Fig. 18. Liew's *Attacking Case* metric for OA and DA for various transmission power strategies when the number of STAs increase.

In Fig. 16, as the number of STAs increases, the amplitude of improved *Attacking Case* increases for all the setups. When minimum transmission power approach is used, the *Attacking Case* for the 3 setups is reduced compared with the default transmission power setup for both OA and DA. For example, for the network with 36 STAs the *Attacking Case* is reduced by 22% for network using DA with minimum transmit power per interface setup compared with DA using default transmit power setup. This is because the transmission power reduction assists to reduce the amount of interference in the network. When comparing the 3 minimum transmit power setups we can observe, as expected, that the minimum transmit power per interface is the most attractive setup followed by minimum transmit power per node, and minimum transmit power per network. This shows our improved *Attacking Case* metric is useful to quantize the severity of interference in networks where various transmission powers are used.

Fig. 17 , as the number of STAs increases the throughput is constant for OA but DA has higher throughput although the slope of the throughput line decreases for all the setups. The throughput is higher when minimum transmission power approach is used for both type of antennas. For example, for the network with 36 STAs the throughput observed for the network using DA with minimum transmit power per interface setup is 16% higher than the throughput obtained on the equivalent network with DA using default transmit power. This is because the transmission power reduction reduces interference in the network as reflected by the improved *Attacking Case* metric in Fig. 16 and this allows more packets to be transmitted per second. For OA, minimum transmit power per network has no significant throughput gain than default transmit power. This is because the transmission power reduction approach is unable to reduce sufficient interference as shown in

Fig. 16. Hence the throughput did not increase greatly. Nevertheless, for the network with 36 STAs the throughput observed for the network using OA with minimum transmit power per node setup is 35% higher than the throughput obtained on the equivalent network with OA using default transmit power.

We can observe in Fig. 18 that the value of Liew's *Attacking Case* increases with the increase of the number of STAs due to the higher accumulation of interference in the network. However the lines of various transmission power setups are similar with one another suggesting all these setups have the same severity of interference in the network and potentially lead to similar aggregated throughput. But the result in Fig. 17 shows the various transmission power setups majorly have different aggregated throughput.

Liew's *Attacking Case* in Eq. 25 consists of components in Eq. 27 (Component 1), Eq. 28 (Component 2) and Eq. 29 (Component 3). Table 2 shows the values for these components for the example of network with 36 STAs. As the sum of i-edges, and rc-edges that are not part of tc-edges and i-edges increases, the sum of tc-edges that are not part of i-edges reduces at similar rate. This causes similar *Attacking Case* values irrespective of the transmission power reduction approach used for each type of antenna.

$$\sum_{\substack{i,j \in V \\ i \neq j}} \left[\mathbb{1}_{[e_{i,j} \in E_I]} \right] \tag{27}$$

$$\sum_{\substack{i,j \in V \\ i \neq j}} \left[\mathbb{1}_{[e_{i,j} \in E_{TC} \wedge e_{i,j} \notin E_I]} \right] \tag{28}$$

$$\sum_{\substack{i,j \in V \\ i \neq j}} \left[\mathbb{1}_{[e_{i,j} \in E_{RC} \wedge e_{i,j} \notin E_{TC} \wedge e_{i,j} \notin E_I]} \right] \tag{29}$$

The improved *Attacking Case* in Eq. 23 consists of components in Eq. 30 (Component 1), Eq. 31 (Component 2) and Eq. 32 (Component 3). Table 3 shows the values of these components for the same network. It shows dissimilar values of *Attacking Case* compare with Table 2. The improved *Attacking Case* metric is able to represent the changes in the aggregated throughput in Fig. 17 more accurately. This shows the usage of weight of edges $w(e_{ij})$ is important to model the severity of interference in networks where various transmission powers are used.

$$\sum_{\substack{i,j \in V \\ i \neq j}} \left[w_I(e_{i,j}) \times \mathbb{1}_{[e_{i,j} \in E_I]} \right] \tag{30}$$

$$\sum_{\substack{i,j \in V \\ i \neq j}} \left[w_{TC}(e_{i,j}) \times \mathbb{1}_{[e_{i,j} \in E_{TC} \wedge e_{i,j} \notin E_I]} \right] \tag{31}$$

$$\sum_{\substack{i,j \in V \\ i \neq j}} \left[w_{RC}(e_{i,j}) \times \mathbb{1}_{[e_{i,j} \in E_{RC} \wedge e_{i,j} \notin E_I]} \right] \tag{32}$$

Comparing the 3 minimum transmit power setups, the power control per interface has the least interference in the network

Table 3
The components of Eq. 23 and the resultant *Attacking Case* using Improved method when the number of STAs is 36.

Method	Setup	Component 1 (Eq. 30)	Component 2 (Eq. 31)	Component 3 (Eq. 32)	AC_{Imp}
OA	DP-Nchan	1040.7	1573.1	1569.8	5224.1
	MP-PNetw	1040.7	1484.1	1536.7	5102.2
	MP-PNode	1052.8	993.3	1066.7	4165.6
DA	DP-Nchan	337.4	537.2	631.3	1843.3
	MP-PNetw	337.4	489.4	601.0	1765.2
	MP-PNode	332.7	362.7	450.8	1478.8
	MP-Pinte	329.8	338.4	424.8	1422.6

and, as a consequence, it leads to the highest aggregated network throughput. Then it is followed by power control per node, and power control per network. The default transmission approach is the least attractive setup. The additional degree of controlling power by interface in DA makes it more attractive than OA. In conclusion reducing *Attacking Case* can result in a potentially increase of throughput. The reduction of *Attacking Case* can be achieved by using strategies such as DA, transmission power reduction, or DA with transmission power reduction.

We have shown that Liew's *Attacking Case* metric is not adequate for networks with nodes using DA; hence the need for a new *Attacking Case* metric. We have also shown that our improved *Attacking Case* supports nodes using DA and it is compatible with nodes using OA; the improved *Attacking Case* metric is able to distinguish the severity of interference by network using nodes with DA and OA. Lastly, we have shown that our improved *Attacking Case* can be used to quantize the interference in networks that use various transmission power schemes.

6. Conclusions

Interference is a fundamental issue in wireless networks and it affects the aggregated throughput of a network. In this paper we have characterized the power interference in IEEE 802.11 CSMA/CA based networks using DA. An improved *Attacking Case* metric that quantizes the severity of interference has been proposed using the Link-Interference Graph, Transmitter-side Protocol Collision Prevention Graph, and Receiver-side Protocol Collision Prevention Graph. This metric differs from Liew' *Attacking Case* metric proposed in [1] as the original metric only addresses networks using OAs. Our improved *Attacking Case* metric is meant for networks using DA but it can also be used in networks using OA. Our proposed *Attacking Case* metric is pertinent as there are no metric available currently to quantize the severity of interference in IEEE 802.11 CSMA/CA based networks using DA. It was also found that interference is tied with *Attacking Case*, thus reducing *Attacking Case* can result in an increase of throughput. The reduction of *Attacking Case* can be achieved by the usage of strategies such as DA, transmission power reduction, or DA with transmission power reduction. The relationship between *Attacking Case* and the throughput of a network is worth to be studied; if there is a statistically strong relationship between these two, a model could be built which is useful to predict the throughput of a network once its *Attacking Case* is calculated. The prediction model would be of assistance in the planning process of a network. This activity remains as our future work.

It would be beneficial to use *Attacking Case* to predict the throughput as the *Attacking Case* metric could be calculated using simple procedure with the knowledge of node positions, transmission power, signal to interference ratio and radio propagation rather than using a discrete event network simulator. Network simulators demand simulator specific codes to be developed, multiple simulations to be executed, wait for the simulations to be completed, and output logs to be analyzed; only then one would have the knowledge on the expected throughput. As a result of this, the computation of the improved *Attacking Case* metric can be easily scaled up beyond the proposed simulation scenario.

References

[1] I.-H. Ho, S.C. Liew, Impact of power control on performance of IEEE 802.11 wireless networks, IEEE Trans. Mobile Comput. 6 (11) (2007) 1245–1258, doi:10.1109/TMC.2007.1045.

[2] IEEE, 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, IEEE Std 802.11–2012 (Revision of IEEE Std 802.11–2007) (2012) 1–2793.10.1109/IEEESTD.2012.6178212

[3] M. Adeyeye, P. Gardner-Stephen, The village telco project: a reliable and practical wireless mesh telephony infrastructure, EURASIP J. Wireless Commun. Netw. 2011 (1) (2011) 78, doi:10.1186/1687-1499-2011-78.

[4] D. Irwin, N. Sharma, P. Shenoy, M. Zink, Towards a virtualized sensing environment, in: T. Magedanz, A. Gavras, N. Thanh, J. Chase (Eds.), Testbeds and Research Infrastructures. Development of Networks and Communities, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 46, Springer Berlin Heidelberg, 2011, pp. 133–142, doi:10.1007/978-3-642-17851-1_10.

[5] E. Anderson, C. Phillips, G. Yee, D. Sicker, D. Grunwald, Challenges in deploying steerable wireless testbeds, in: T. Magedanz, A. Gavras, N. Thanh, J. Chase (Eds.), Testbeds and Research Infrastructures. Development of Networks and Communities, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 46, Springer Berlin Heidelberg, 2011, pp. 231–240, doi:10.1007/978-3-642-17851-1_19.

[6] V. Kapnadak, M. Senel, E.J. Coyle, Low-complexity, distributed characterization of interferers in wireless networks, Int. J. Distrib. Sensor Netw. 2011 (2011) 17, doi:10.1155/2011/980953.

[7] R. Karrer, A. Pescape, T. Huehn, Challenges in second-generation wireless mesh networks, EURASIP J. Wirel. Commun. Netw. 2008 (1) (2008) 274790, doi:10.1155/2008/274790.

[8] S. Kandasamy, R. Campos, R. Morla, M. Ricardo, Using directional antennas on stub wireless mesh networks: impact on throughput, delay, and fairness, in: Proceeding of the 19th International Conference on Computer Communications and Networks (ICCCN), 2010, pp. 1–6, doi:10.1109/ICCCN.2010.5560027.

[9] S. Kandasamy, R. Campos, R. Morla, M. Ricardo, Improving the performance of ieee802.11s networks using directional antennas over multi-radio/multi-channel implementation - the research challenges, in: Proceeding of the 4th Doctoral Symposium on Informatics Engineering (DSIE), 2009, pp. 1–12.

[10] R. Moraes, F. Arajo, Modeling interference in wireless ad hoc networks, in: Proceeding of the 15th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS), 2007, pp. 54–59, doi:10.1109/MASCOTS.2007.38.

[11] Y. Liu, X. Zhang, Q. Liu, S. Dai, Interference-aware physical carrier sensing for maximum throughput in ad hoc networks, in: Proceeding of the 3rd International Conference on Communications and Networking in China (ChinaCom), 2008, pp. 60–64, doi:10.1109/CHINACOM.2008.4684969.

[12] Z. Zeng, Y. Yang, J. Hou, How physical carrier sense affects system throughput in ieee 802.11 wireless networks, in: Proceeding of the 27th IEEE Conference on Computer Communications (INFOCOM), 2008, pp. 1445–1453, doi:10.1109/INFOCOM.2008.203.

[13] S. Varma, V. Tokekar, An interference graph based MAC protocol for multi rate ad hoc networks, in: Proceeding of the World Congress on Information and Communication Technologies (WICT), 2011, pp. 581–586, doi:10.1109/WICT.2011.6141310.

[14] T.-M. Hoang, M. Hoang, Q.-B. Nguyen, A novel computation for supplementing interference analytical model in 802.11-based wireless mesh networks, in: Proceeding of the 8th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), 2012, pp. 1–4, doi:10.1109/WiCOM.2012.6478324.

[15] M. Parvej, S. Chowdhury, N. Hia, M. Uddin, Capture effect on the optimal contention window in ieee 802.11 based WLANs, in: Proceeding of the International Conference on Informatics, Electronics Vision (ICIEV), 2013, pp. 1–5, doi:10.1109/ICIEV.2013.6572592.

[16] P. Gupta, P. Kumar, The capacity of wireless networks, IEEE Trans. Inf. Theory 46 (2) (2000) 388–404, doi:10.1109/18.825799.

[17] P.C. Ng, S.C. Liew, L.B. Jiang, A performance evaluation framework for ieee 802.11 ad-hoc networks, in: Proceeding of the 1st ACM International Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks (PE-WASUN), ACM, New York, NY, USA, 2004, pp. 123–124, doi:10.1145/1023756.1023781.

[18] B. Alawieh, C. Assi, H. Mouftah, Investigating the performance of power-aware ieee 802.11 in multihop wireless networks, IEEE Trans. Veh. Technol. 58 (1) (2009) 287–300, doi:10.1109/TVT.2008.924971.

[19] I. Tinnirello, G. Bianchi, Interference estimation in ieee 802.11 networks, IEEE Control Syst. 30 (2) (2010) 30–43, doi:10.1109/MCS.2009.935570.

[20] L. Fu, S.C. Liew, J. Huang, Effective carrier sensing in CSMA networks under cumulative interference, IEEE Trans. Mobile Comput. 12 (4) (2013) 748–760, doi:10.1109/TMC.2012.45.

[21] P. Li, C. Zhang, Y. Fang, The capacity of wireless ad hoc networks using directional antennas, IEEE Trans> Mobile Comput. 10 (10) (2011) 1374–1387, doi:10.1109/TMC.2010.243.

[22] K. Xu, B. Garrison, K.-C. Wang, Performance modeling for IEEE 802.11 vehicle-to-infrastructure networks with directional antennas, in: Proceeding of the IEEE Vehicular Networking Conference (VNC), 2010, pp. 215–222, doi:10.1109/VNC.2010.5698259.

[23] S. Yi, Y. Pei, S. Kalyanaraman, On the capacity improvement of ad hoc wireless networks using directional antennas, in: Proceeding of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), ACM, New York, NY, USA, 2003, pp. 108–116, doi:10.1145/778415.778429.

[24] B. Alawieh, C. Assi, W. Ajib, Distributed correlative power control schemes for mobile ad hoc networks using directional antennas, IEEE Trans. Veh. Technol. 57 (3) (2008) 1733–1744, doi:10.1109/TVT.2007.909264.

[25] The Network Simulator NS-2. (http://www.isi.edu/nsnam/ns/).