Distributed range assignment for reliable channel access and reuse in ad-hoc networks

G. Srivastava  
*University of Wollongong*, gauravs@uow.edu.au

P. Boustead  
*University of Wollongong*, boustead@uow.edu.au

Joe F. Chicharo  
*University of Wollongong*, chicharo@uow.edu.au

Publication Details  
Distributed range assignment for reliable channel access and reuse in ad-hoc networks

Abstract
The available bandwidth in an ad-hoc network can decrease rapidly due to the shared access to the communication channel. Power control can enhance the available bandwidth by allowing non-interfering nodes to communicate simultaneously. A number of power aware topology control algorithms have been proposed, where low power transmissions are used to forward data. However, evaluating the power level for the data packets is not sufficient. Reliable transmission of the data packets in a shared channel network requires a number of signalling messages at the Medium Access Channel (MAC) layer. The transmission power of the signalling messages is crucial for both reliable access and channel reuse. We propose a distributed range assignment algorithm (DRA), that can be applied to a power aware topology control algorithm. to evaluate an appropriate power for the signalling messages. A worked example and a simulation based analysis of DRA, applied to a Distributed Relative Neighbourhood Graph is provided. Furthermore, a study on the impact of the transmission range, on the power usage and channel reuse is conducted.

Disciplines
Physical Sciences and Mathematics

Publication Details

This conference paper is available at Research Online: http://ro.uow.edu.au/infopapers/260
DISTRIBUTED RANGE ASSIGNMENT FOR RELIABLE CHANNEL ACCESS AND REUSE IN AD-HOC NETWORKS.

Gaurav Srivastava, Paul Bousted, Joe F. Chicharo

School of Electrical, Computer and Telecommunication Engineering, University of Wollongong, NSW, Australia.
Email: gaurav@titr.uow.edu.au, paul@titr.uow.edu.au, Joe.chicharo@elec.uow.edu.au

ABSTRACT

The available bandwidth in an ad-hoc network can decrease rapidly due to the shared access to the communication channel. Power control can enhance the available bandwidth by allowing non-interfering nodes to communicate simultaneously. A number of power aware topology control algorithms have been proposed, where low power transmissions are used to forward data. However, evaluating the power level for the data packets is not sufficient. Reliable transmission of the data packets in a shared channel network requires a number of signalling messages at the Medium Access Channel (MAC) layer. The transmission power of the signalling messages is crucial for both reliable access and channel reuse. We propose a distributed range assignment algorithm (DRA), that can be applied to a power aware topology control algorithm, to evaluate an appropriate power for the signalling messages. A worked example and a simulation based analysis of DRA, applied to a Distributed Relative Neighbourhood Graph is provided. Furthermore, a study on the impact of the transmission range, on the power usage and channel reuse is conducted.

1. INTRODUCTION

An ad-hoc network is a group of wireless nodes working together to form a network. Each network node can act as a router and forward traffic. The origin of ad-hoc networks dates back to 1970s, with the introduction of packet radio networks [1]. A packet radio network used the basic carrier sensing mechanism, Carrier Sense Multiple Access (CSMA), to gain access to the communication channel [1]. A node executing CSMA is unable to detect the communication beyond it’s sensing range [1]. Therefore, nodes out of the transmission range of a transmitter are hidden, and can cause collisions at a receiver by transmitting at the same time. This problem is known as the Hidden node problem and initially studied in [2].

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), has been proposed to improve the carrier sensing mechanism in a CSMA based network [3]. In CSMA/CA, reliable data transmission is achieved by a number of signalling messages exchanged by a transmitter and a receiver node. The IEEE 802.11 standard has been proposed on the CSMA/CA MAC protocol [4].

A number of power aware topology control algorithms have been proposed for ad-hoc networks [5] [6] [7] [8]. These algorithms model a network topology as a Graph $(V, E)$, of vertex set $V$ and edge set $E$. A vertex represents a network node and an edge represents a link between two nodes. A graph is connected if there is a path between every pair of nodes. A comparison of the algorithms is provided in [9][10]. The power aware topology control algorithms aim to establish a connected graph with minimum transmission power. The algorithms use power control at each node to transmit data based on the length of an edge between the two nodes, thereby improving the performance of a network in two ways: (1) The overall power consumption is reduced as the transmission power is adjusted to cover the link distance between two nodes and minimum power routes are evaluated to forward the data packets, and (2) Low power communications reduce the communication interference and allowed non-interfering nodes to communicate simultaneously.

In a CSMA/CA based network, low power communication doesn’t necessarily increase the ability to reuse the communication channel as the protocol uses a number of signalling messages to allocate the range of channel reservation. If the power derived from executing a power aware topology control algorithm is directly used for the signalling messages, a number of hidden nodes may arise [11]. Using the maximum power for the signalling messages will reduce the hidden nodes but will also reserve the channel over the maximum range and decrease the ability to reuse the channel for other communications.

In this paper we propose a distributed range assignment algorithm (DRA), to evaluate an appropriate power for the signalling messages, Request-To-Send (RTS) and Clear-To-Send (CTS) used in CSMA/CA MAC protocol. The power of the RTS and the CTS messages is calculated from the one hop link state information of a transmitter and a receiver node. As a result, a network is able to support low power communications and promote the reuse of the communication channel. The proposed algorithm can be applied to a number of graph based topology control algorithms, including a Relative Neighbourhood Graph (RNG) [5] and Minimum Spanning Tree (MST) [6].

The remainder of the paper is organised as follows. Section 2 of the paper outlines the literature on MAC protocols. Section 3 outlines the channel reuse and power control issues related to topology control and the CSMA/CA MAC. In Section 4 we propose DRA. In Section 5, a worked example is provided to illustrate the operational aspects of DRA. Section 6, provides a simulation based analysis of DRA. Section VII concludes the paper.

2. BACKGROUND

2.1. Channel Access Mechanisms

MAC protocols perform a number of vital functions such as channel access to a shared medium and reliable data transfer. A MAC protocol provides an interface to the Physical layer and acts as a...
buffer between the Network and the Physical layer. CSMA is a channel access technique, where each node senses the channel before transmission. Collisions are avoided by not transmitting in a busy channel. A significant number of MAC protocols are based on CSMA approach [12][13][3][14]. In CSMA, nodes undertake a binary or exponential backoff, on sensing a busy channel [3]. The most significant problem in a common channel CSMA MAC protocol is the Hidden Node and the Exposed Node problem [2].

Hidden Node arises when two nodes are attempting to communicate with a common node and are unable to sense the carrier form each other. In Figure 1(a), nodes A and C are attempting to transmit a frame to node B. Node A and C's carrier sense finds the channel to be clear and therefore transmit simultaneously. This results in a packet collision at the receiver node B.

Exposed Node problem arises when a transmission from node B to A, prevents the transmission of node C to D, although D is out of the transmission range of node B. This scenario is shown in Figure 1(b). Since nodes B and C are in each others sensing range, both node sense the carrier as busy. Node C should be able to transmit to node D without colliding with the transmission from B to A.

In order to solve the Hidden Node problem, a signalling mechanism was proposed in CSMA/CA [2]. CSMA/CA protocol is based around control message handshake between the transmitter and the receiver. In CSMA/CA protocol, a transmitter node initially sense the channel by first listening for existing transmissions. If the carrier is busy, a node will delay its transmission. The delay in transmission is based on a backoff procedure [2]. However, if the carrier is not busy, a handshake between a transmitter and a receiver is executed. A transmitter is always required to transmit a RTS packet in order to transmit a data packet. A receiver acknowledges with a CTS reply. A data packet is then transmitted by a transmitter and a receiver replies with a ACK packet to confirm the reception. If the frame is not received or the Cyclic Redundancy Check (CRC) fails, then a retransmission occurs.

3. CHANNEL REUSE AND POWER CONTROL

In a CSMA/CA based network, the power level used for the RTS and the CTS packets, will determine the region for which the channel is reserved. If RTS and CTS messages are exchanged at the maximum power, all network nodes in the region covered by the broadcast (node with the transmission range of a transmitter and a receiver) will need to delay access to the channel. The nodes covered by a RTS or a CTS (apart from the receiver and the transmitter), would not be able to communicate at the same time. In a dense network, a high transmission power can cover a large number of nodes, introducing a large number of Exposed nodes. Since the Exposed nodes will not be able to transmit, the available bandwidth can decrease significantly. A theoretical and experimental study in [15][16], examines the effect of the exposed nodes on the available bandwidth. In a shared channel network, the available bandwidth can decrease rapidly in the order of $O(1/\sqrt{N})$, where $(N)$ are the number of network nodes [15][16]. In order to provide spatial reuse, it is necessary to reduce the number of Exposed nodes.

Network nodes can alter the transmission power to control the range of a transmission. A signal attenuation model for transmission power of a signal is proposed in [17]. The model relates the effect of the signal propagation on distance. The transmission power $(P_t)$, attenuates over distance $d$ and is calculated by using Equation 1.

$$P_r = P_t + 10 \log \left( \frac{d^2}{d^2 + d_0^2} \right)$$

Where, $P_r$, is the received power, $d$ is the speed of light, $f$ is the frequency of the spectrum and $\lambda$ is the signal attenuation factor, which depends on the transmission medium. If nodes are using an omni-directional antenna, transmission from one network node can interfere with the communications of many other network nodes within it's transmission range. A collision occurs at a receiver when the signal to noise ratio is below a threshold value. A node can adjust the magnitude of signal interference by adjusting it's transmission power. A low power transmission will result in a low interference on other network communications. In a power aware topology control algorithm, the power level used for the data packets cannot be directly used for signalling messages, as a number of interfering nodes (hidden from communication) may exist and can disrupt the communication between a transmitter and a receiver. Removal of hidden nodes is necessary to avoid packet collisions and provide a reliable access to the communication channel. In order to illustrate the hidden node and the exposed node problem, we examine a Distributed Relative Neighbourhood Graph (DRNG) based network topology. DRNG is a distributed topology control algorithm to calculate a RING [5]. DRNG are exactly those nodes $i, j$ where there is no node z (within the transmission range of node i and j), such that $|r_{iz} - |r_{ij}|$ and $|r_{iz}| < |r_{ij}|$ where, $r_{ij}$ denotes the distance between nodes i and j.

Figure 2(a) and 2(b) are graph representations of a DRNG based topology. The lines represent a link between the nodes and the concentric circles represent the transmission range. In Figure 2(a), the transmission power of the RTS and the CTS packets is based on the link distance of the transmitter and the receiver. In Figure 2(b), the maximum transmission power is used for the RTS and the CTS messages. For example, in Figure 2(a) and 2(b), nodes 1, 5 and 6 want to communicate with nodes 2, 3 and 4, denoted by $\{1 \rightarrow 2, 5 \rightarrow 4\}$ and $\{6 \rightarrow 3\}$. In Figure 2(a), node 1 will send a RTS to node 2 to cover the link distance $r_{12}$. Node 2 will reply with a CTS to cover the same link distance $r_{12}$. The power of the communication between node 1 and 2 is not large enough to reach node 5. Node 5 is hidden from the communication, and any transmission from node 5 to node 4, can cause a collision at node 2.
Hence the communication \{1 \rightarrow 2\}, in Figure 2(a), is not reliable as it can be easily disrupted by node 5. In Figure 2(b), node 1 will transmit a RTS at the maximum power which will be received by nodes \{2, 5, 6\}. Node 2 will reply with a CTS at the maximum power which will reach nodes \{1, 4, 5\}. Therefore, nodes 5 and 6 will differ access to the transmission channel. If node 5 acquires the channel first, a RTS by node 5 at the maximum power will reach nodes \{1, 2, 4, 6\}, and nodes 1 and 6 will delay their access to the channel. If node 6 acquires the channel first, a RTS by node 6 at the maximum power will reach nodes \{1, 4, 5\}, and nodes 1 and 6 will delay their access to the channel. Hence, in Figure 2(b), only one out of the three communications can occur at the same time.

Traffic can originate at any part of the network and there is no guarantee that node 5 may not need to communicate with node 4. Therefore, all probable interfering nodes need to be considered to evaluate an appropriate power level for a RTS and a CTS message handshake.

4. PROPOSED ALGORITHM

In DRA, the transmission power of a RTS and a CTS packets is evaluated on the basis of the one hop maximum power link-sate information of a transmitter and a receiver node. In order to eliminate the Hidden Nodes on a particular link, the power of a RTS and a CTS packet is set to cover all nodes that can interfere with the communication of a transmitter and a receiver. This is different to the power assignment in a topology control algorithm, where the transmission power is adjusted to reach a receiver node.

In DRA, we require a distributed topology construction and dissemination mechanism. A neighbour discovery mechanism similar to “Hello” message [18], is used to construct and disseminate the one hop link-sate information among the network nodes. A “Hello” packet contains a node’s identification address and is transmitted by a node to broadcast it’s existence in a network. A node receiving a “Hello” transmission determines the nodes located in it’s neighbourhood. The identification address included in a “Hello” packet is stored in a list \(N_i\). A node can then execute a particular power aware distributed topology control algorithm to construct a Topology Control Neighbour (TCN) list from the nodes in \(N_i\). Nodes can further exchange the TCN list in a distributed manner by attaching the TCN list to the “Hello” packets. The exchange of TCN information is important to evaluate the local topology of a neighbouring node. The maximum interference introduced by a node depends on the power used to communicate with it’s furthest TCN node. A node can evaluate its neighbour’s furthest TCN by iterating through its neighbour’s TCN list.

In order to evaluate a list of interfering nodes a transmitter ‘i’, calculates the distance to a receiver ‘k’. Node ‘i’ then iterates through \(N_i\). For each node ‘j’ in \(N_i\), the distance between ‘j’ and ‘k’ \(r_{jk}\) is calculated and compared with \(r_{jfn}\), which is the distance between ‘j’ and its furthest TCN neighbour ‘fn’. The condition that node ‘j’ can interfere with the communication between node \{i \rightarrow k\} if, \(r_{jfn}\) is greater or equal to \(r_{jfk}\). If node ‘j’ is closer to a transmitter ‘i’ as compared to a receiver ‘k’, node ‘j’ is added the \(TCN_{backoff}\) list of node ‘i’.

A receiver uses the same process to evaluate the interfering nodes. Node ‘j’ is added to the \(TCN_{backoff}\) list of a receiver node ‘k’, if the distance between ‘j’ and ‘k’ is closer to ‘k’ than ‘i’. A transmitter initialises the \(TCN_{backoff}\) list to include a receiver node. A receiver, initialises the \(TCN_{backoff}\) list to include a transmitter node. The power of a RTS or a CTS packet is set to reach the furthest node in the \(TCN_{backoff}\) list. This process is illustrated in the SET-RTS-CTS-RANGE() function.

Algorithm SET-RTS-CTS-RANGE()

1. if PACKET TYPE = RTS
2. then \(i\) --Transmitter node
3. \(k\) --Receiver node
4. if PACKET TYPE = CTS
5. then \(i\) --Receiver node
6. \(k\) --Transmitter node
7. \(N_i\) --Max power neighbour list of node \(i\)
8. \(r_{ij}\) --The distance between node \(i\) and \(j\)
9. \(TCN_{backoff}\) --The backoff list of node \(i\)
10. if \(N_i\) \(\neq\) 0
11. for each node \(j\) in \(N_i\)
12. \(f_n\) --is the furthest TCN node of \(j\)
13. if \(r_{jfn} \geq r_{jk}\) AND \(r_{ij} \leq r_{jfk}\)
14. then Add \(j\) to \(TCN_{backoff}\)
15. for each node \(j\) in \(TCN_{backoff}\)
16. \(f\) --the furthest node in \(TCN_{backoff}\)
17. return \(r_{ij}\)

5. WORKED EXAMPLE

In this section we illustrate the working of DRA applied to a DRNG based network topology initially proposed in Figure 2(a). Figure 3, is a graphical representation of DRA applied to a DRNG based topology. The solid lines represent an edge between the nodes and the dotted concentric circles illustrate the power used by the RTS and the CTS messages.

The one hop neighbours of node 1 are given by \(N_1 = \{2, 5, 6\}\). Node 5, can interfere with the transmission of node \{1 \rightarrow 2\}, as the furthest TCN neighbour of node 5 is 4 and \(r_{54} > r_{52}\). Since \(r_{51} < r_{52}\), node 5 is closer to node 1 and is added to the \(TCN_{backoff}\) list of node 1. In the case of node 2, the one hop
neighbours are given by \( N_2 = \{1, 5, 4\} \). Nodes \{5, 4\} can interfere at node 2, hence the \( TCN_{\text{backoff}} \) list of node 2 includes nodes 4 and 5. The furthest node in the \( TCN_{\text{backoff}} \) list of node 2 is node 4. The power of the RTS issued by node 1 is set to reach node 5 and the power of the CTS issued by node 2 is set to reach node 4. In the case of \{6 \rightarrow 3\} the one hop neighbour of node 6 that can cause interference is 5 as \( r_{65} > r_{63} \). Since \( r_{65} < r_{63} \), node 5 is added to the \( TCN_{\text{backoff}} \) list of node 6 and the RTS issued by node 6 is set to reach node 5. The CTS power level of node 3 is set to include node 6 only, as \( r_{35} > r_{36} \). Therefore, nodes 1 and 2 can communicate at the same time as nodes 6 and 3, which was not possible in the case of MPT.

6. SIMULATION AND ANALYSIS

6.1. Scenario

A simulation based study of topology graphs is conducted to examine the effect of the transmission range and the number of network nodes on a DRNG topology. A simulation is used to analyse three scenarios, MPT, DRA and DRNG. A number of transmission range values are examined \{100m, 150m, 200m\}. The nodes are distributed randomly in a 600mx600m grid area and varied in number from 10 to 100. The simulation results are averaged over 1000 random seeds. The power in mW is given by \( P_{\text{avg}}(\text{mW}) = 10^{(P_{\text{avg}}(\text{dBm})/10)} \), where \( P_{\text{avg}}(\text{dBm}) \) is calculated by using Equation 1.

The hidden and the exposed nodes are evaluated for every link in a topology graph. The performance metrics studied are as follows: (a) Average RTS and CTS power, which is defined as the average power used for the RTS and CTS packet per link. (b) Average hidden nodes, which is defined as the ratio of the total number of hidden nodes over the total number of links in a network. (c) Average exposed nodes, which is defined as the ratio of the total number of exposed nodes over the total number of links in a network.

6.2. Results

The total number of links in DRA, MPT and DRNG are the same for a particular transmission range, as only the power of a RTS and a CTS packet is modified. In the simulation, a linear increase in the number of links is observed with an increase in the number of nodes. This result is also verified in [10].

Figure 4(a), is a plot of the average power used by the RTS and CTS packets per link, against the total number of network nodes. In MPT, the average power per link for a particular transmission range is fixed, as all RTS and CTS packets are transmitted at the maximum transmission range. In MPT, an average power of approximately \(3.2\text{mW}, 1.8\text{mW}, 1.25\text{mW}, 0.8\text{mW} \) is observed for the transmission range values of \{200m, 150m, 125m, 100m\} respectively. DRA and DRNG both illustrate a drop in the average transmission power of the RTS and the CTS packets, with an increase in the size of the network. In DRA, as the size of the network is increased from 10 to 100 nodes, the average power of the RTS and the CTS packets decreases \{\approx 73\%, 56\%, 41\%, 24\%\} of its maximum value, for the transmission range values of \{200m, 150m, 125m, 100m\} respectively. In DRNG, the average power of the RTS and CTS packets decreases \{\approx 82\%, 73\%, 63\%, 50\%\} of its maximum value. In a 100 node network, the average power used in DRA is \approx \{63\% - 86\%\} higher than a DRNG based network topology for the transmission range values examined.

Figure 4(b) is the plot of the average hidden nodes per link against the number of network nodes. Figure 4(b), illustrates that at a node density of \approx 100 nodes, there are \approx 14-16 hidden nodes for every 10 links in a DRNG based network topology. Figure 4(b) illustrates that there are no hidden nodes in the case of a DRA and a MPT based network topology.

Figure 4(c) is a plot of the average exposed nodes per link against the number of network nodes. In MPT, the average number of exposed nodes are significantly higher than DRA and DRNG. Figure 4(c) illustrates that at a node density of \approx 100 nodes, the number exposed nodes per link in DRA are \approx \{50\%-80\%\} lower than MPT. In the case of DRA and DRNG, the average exposed nodes increase with an increase in the number of network nodes. In a network of \approx 100 nodes, the average exposed nodes in a DRNG topology are \approx \{50\%\} lower than DRA.

In summary, the simulations indicate that the RTS and the CTS power assignments based on the link distance in a DRNG topology is not sufficient, and a number of hidden nodes may arise. Such hidden nodes can be reduced by applying DRA or exchanging the RTS and the CTS at the maximum transmission power. However, the power used in MPT is significantly higher than DRA. Another disadvantage of MPT is observed in the number of exposed nodes. In MPT, the total number of exposed nodes are significantly higher than DRA and DRNG, which restricts the ability to reuse the communication channel.

7. CONCLUSION

In this paper we have proposed a distributed algorithm which can be applied to a number of power aware topology control algorithm to adjust the transmission power of the RTS and the CTS messages. As a result, DRA is able to reduce the hidden nodes and promote channel reuse in a CSMA/CA network. A worked example and a simulation based analysis of DRA is provided. An ideal case is considered in this simulation.

8. REFERENCES


