Department of Electrical and Computer Engineering

A Multichannel Medium Access Control And Its Performance Estimation For Multihop Wireless Sensor Networks

Prihadi Murdiyat

This thesis is presented for the Degree of Doctor of Philosophy of Curtin University

March 2018

DECLARATION

To the best of my knowledge and belief, this thesis contains no material previously published by any other person except where due acknowledgement has been made.

This thesis contains no material which has been accepted for award of any other degree or diploma in any university.

Signature : ……………………………..

Date : …………………………

ABSTRACT

Nowadays, Wireless Sensor Networking (WSN) still attract much research due to its advantages for many more applications. WSN is not only deployed in urban areas, but in rural areas where telecommunication and main power infrastructures may not be available. An example of WSN located in rural area is an environmental monitoring WSN studied in this thesis. This system is developed to give an early warning for people living in disaster prone areas in the Province of East Kalimantan, Indonesia, where flash floods, landslides, and forest fires often occur.

This thesis studies a large scale WSN consisting groups of sensor nodes (SNs) that are mostly located in rural area. A control station (CS) that provides network supervisory and management is located in the capital city separated hundreds kilometres away from the rural area. As the system comprises a large number of SN groups dispersed in many locations within the province, a three-tier dedicated WSN infrastructure is utilized to provide communication between SN groups and CS. Tier 1, that is the lowest tier of the network, consists of SNs which are responsible for collecting and reporting local data to the CS. On the other hand, Tier 2 and Tier 3 are purposed to relay reported data to the CS. To establish communication links within hostile propagation environments in often mountainous rural areas, the proposed three-tier multi-hop network offers a flexible solution.

Nevertheless, employing multi-hop network is challenging as the network suffers performance degradation due to hidden and exposed node problems. Reliable and efficient operations of Tier 2 and Tier 3 are critical in ensuring the performance of such a multihop network. This thesis proposes a multichannel MAC, called 2-Hop Channel Reservation (2HCR), to improve the performance of Tier 2 and Tier 3, which are configured as long chain multihop networks in tree topology. In an effort to reduce the detrimental effect on network performance caused by the hidden and exposed node problems, 2HCR protocol ensures that nodes located two hops away from a transmitting node to adopt a different channel frequency for their transmissions. The performance of the proposed 2HCR protocol has been evaluated

and compared with multichannel CSMA (MC CSMA) [40] and 802.11b [18], the latter being commonly used for the study of performance in multihop networks. Meanwhile, MC CSMA is chosen as it has a similar mechanism with 2HCR. Computer simulation shows that 2HCR achieve an average throughput 2.53 times higher than that of 802.11b. Meanwhile, the average throughput of MC CSMA is only 2.12 times higher than that obtained with 802.11b protocol. 2HCR has a better performance than MC CSMA as it provides a better channel use distribution.

Computer simulation is commonly used to evaluate the performance of WSN. Also, several methods have been proposed for estimating network performance in the literature. A number of these schemes [33-35] are reviewed in this thesis for their suitability in predicting throughputs for networks in Tier 2 and Tier 3. However, such estimation methods do not concern about specific topologies, and as such they tend to either under or overestimate the capacity of a given topology. To increase the estimation accuracy, such methods are extended to take into consideration a given specific network topology. Moreover, this will then result in a different formulation and computation for each change in network topology. Instead, a simple estimation method is proposed in this thesis to predict the throughput of any network configuration likely to be considered in Tier 2 and Tier 3. The proposed throughput estimation method involves little computational efforts, thereby making it attractive for field application whenever a change in network configuration is required. The throughputs for a number of different tree topologies estimated using the proposed method are compared with those obtained by computer simulation. It is shown that the estimated and computer simulated throughputs are deviated by less than 10 % when operating with either 2HCR, MC CSMA or 802.11b.

Since the function of network supervisory and management is remotely carried out by the CS, this will reduce the need for sending maintenance staff to service the WSN in isolated rural area. As a result, the attendance time consumption and cost could be significantly reduced. To implement remote network management, instruction packets are regularly sent by CS to individual nodes in the network. Consequently, packet traffic also flows from CS to SN in addition to any existing traffic flowing from SN to CS. In this thesis, traffic travelling from CS to SNs is referred to as reverse traffic while the traffic from SN to CS is called forward traffic.

The influence of the bidirectional traffic on the performance of 2HCR has been evaluated using computer simulation. As for the case with unidirectional traffic, the throughputs achieved with 2HCR involving bidirectional traffic are then compared with those obtained using MC CSMA and 802.11b. For a given topology, it is shown that 2HCR achieves a throughput that is 2.57 times higher than that obtained by 802.11b. On the other hand, the throughput obtained by MC CSMA is 2.41 times better than that of 802.11b.

With bidirectional traffic, further evaluation is provided for 2HCR and 802.11b. The purpose of this evaluation is to observe packet delivery rate of reverse and forward traffics for two situations. In the first situation, i.e., symmetric setting, reverse and forward traffics generate the same data rate, whilst in the second situation, i.e., asymmetric setting, the data rate of reverse traffic is lower than that of forward traffic. The simulation results show that packet delivery rate of reverse and forward traffic is similar in case of symmetric situation. However, in asymmetric situation, packet delivery rate of reverse traffic is below the packet delivery rate of forward traffic. As reverse traffic has an important role to support successful network supervisory and management, packet delivery rate of this traffic must be higher than that of forward traffic. This thesis addresses three attempts to achieve such a requirement. For the first attempt, the existing 802.11e [39] priority scheme is adopted in bidirectional network. In this scheme, a short interframe space (IFS) and contention window (CW) size are assigned to reverse traffic, while the longer IFS and CW size is given to forward traffic. Despite this method increases packet delivery rate of reverse traffic, the reverse traffic packet delivery rate in the second scenario is still lower than the forward traffic packet delivery rate. As the first attempt is not successful, the second attempt utilizes a different strategy. In the second attempt, the throughput of forward traffic is supressed by implementing RTS/CTS mechanism available in 802.11 [18], to reverse traffic. The simulation results show that this method provides a better reverse traffic packet delivery rate than that provided by 802.11e. However, for asymmetric situation, the reverse traffic packet delivery rate is slightly lower than forward traffic packet delivery rate. As previous methods could not give a desired result, another method so called a simple priority support scheme is proposed in this thesis. This method combines the advantage of RTS/CTS and 802.11e based schemes. In this method, RTS/CTS is still implemented for reverse traffic with a short IFS is assigned to reverse traffic to give reverse traffic a high priority to access the channel resource. Simulation results show that reverse traffic packet delivery rate in asymmetric situation is higher than forward traffic packet delivery rate.

ACKNOWLEDGEMENTS

All praises go to Allah All Mighty, who gives me opportunity to study until this level, and provides ways to complete it. There is neither strength nor effort except with Allah.

It is certain that this research would not be completed without advices, encouragements, and assistances from many people. Therefore, first of all, I would like to express my sincere gratitude to my supervisor, Dr. King Sun Chan, for his directions, evaluations, and advices that made me able to finish this study.

I also would also like to express my gratitude and appreciation to my co-supervisor, previously my supervisor, Professor Kah Seng Chung, for his encouragements and expertise. The invaluable lessons have opened and enriched my mind on the philosophy of telecommunication technology and the researcher's attitude.

Furthermore, I appreciate colleagues who were in Communication Technology Research Group. A friendly and supporting environment has made me feel convenient to work along with them. I wish the period that full with hard work can bring us to the better future.

Last but not least, it can be forgotten the continuous supports, prays, and encouragements from my wife, our children, parents, and other family members. These have made me keep working hard to finish my study.

PUBLICATIONS

1. P. Murdiyat, K. S. Chung, and K. S. Chan, "Estimating the network throughput of two channels MAC for multihop wireless networks", in *Proceeding* of TENCON 2016, Singapore, Nov. 22-25 2016.

2. P. Murdiyat, K. S. Chung, and K. S. Chan, "A multi-channel MAC for multi-hop wireless sensor networks minimizing hidden node collision", in *Proceeding of 2016 Asia Pacific Conference on Communication (APCC2016),* Yogyakarta, Indonesia, Aug. 25-27 2016, pp. 535-540.

3. P. Murdiyat, K. S. Chung, and K. S. Chan, "Predicting the network throughput of wide area WSN in rural areas", in *Proceeding of 2014 Asia Pacific Conference on Communication (APCC2014),* Pattaya, Thailand, Oct. 1-3 2014, pp. 106-111.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

2HCR	2 Hops Channel Reservation
ACK	Acknowledgement packet
ADC	Analogue to Digital Converter
ADSL	Asymmetric Digital Subscriber Line
ATIM	Adhoc Traffic Indication Message
ATIM-ACK	Adhoc Traffic Indication Message-Acknowledgement
ATIM-RES	Adhoc Traffic Indication Message-Reservation
BN	Backbone Node
BS	Base Station
BTS	Base Transceiver Station
CDMA	Code Division Multiple Access
CDMAC	Coordinated Directional MAC
CDR-MAC	Circular Directional RTS MAC
CH	Cluster Head
CHMA	Common Hopping Multiple Access
CS	Control Station
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CTB-MAC	Channel Traffic Balance – Multiple Access Control
CTS	Clear To Send
CUL	Channel Usage List
CW	Contention Window
DATA	Data packet
dBi	deci Bell over isotropic antenna
DBTMA	Dual Busy Tone Multiple Access
DCA	Dynamic Channel Assignment
DCC	Dedicated Control Channel
DCF	Distributed Coordination Function
DIFS	DCF Interframe Space
DMAC	Directional MAC
DNAV	Directional Network Allocation Vector

FCL	Free Channel List
GHz	Giga Hertz
GPRS	General Packet Radio Service
GPS	Global Positioning System
H-MMAC	Hybrid Multi-channel Multiple Access Control
ID	Identity
IFS	Interframe space
LH	Local Head
kbps	kilo bits per second
MAC	Multiple Access Control layer
MACA-BI	Multiple Access with Collision Avoidance By Invitation
Mbps	Mega bits per second
MC CSMA	Multi-Channel Carrier Sense Multiple Access
MCDA	Multichannel MAC Protocol with Directional Antenna
Mc MAC	Multi-channel Multiple Access Control
MEM	Micro Electro Mechanical
MHz	Mega Hertz
MMAC	Multi-channel Multiple Access Control
NAV	Network Allocation Vector
NIL	Neighbour Information List
NS3	Network Simulator 3
PHY	Physical layer
PCF	Point Coordination Function
PCL	Preferred Channel List
PIFS	PIFS Interframe Space
PSM	Power Saving Mechanism
QoS	Quality of Service
RES	Reservation
RI-BTMA	Receiver Initiated Busy Tone Multiple Access
RN	Relay Node
RTR	Ready To Receive
RTS	Request To Send
SC	Split Channel
SIFS	Short Interframe Space

SN	Sensor Node
ST	Sensing Threshold
TFN	Transformed Node
TRSS	Total Received Signal Strength
UMTS	Universal Mobile Telecommunication System
VHF	Very High Frequency
W	Watt
WLAN	Wireless Local Area Network
WSN	Wireless Sensor Network

LIST OF SYMBOLS AND NOTATIONS

W	channel capacity (bps)
n	number of nodes in a region
Θ	Knuth's notation for an asymptotic tight bound
Nn	Node n
B_{Tr}	Receive busy-tone
B_{Tt}	Transmit busy-tone
fn	Frequency n
tn	Time n
n	Current hop
n-1	Previous 1 hop
n-2	Previous 2 hop
ch_h	Transmission channel utilized in n-2
ch_i	Transmission channel utilized in n-1
rn31rx	The data rate of packet coming from RN2 (or TFN1) to RN3
rn32rx	The data rate of packet arriving from LH3 at RN3
bn1rx	The data rate of packet at BN which is originally from RN2
bn2rx	The data rate of packet at BN which is originally from LH3
bn tot	The total data rate of packet received by BN

CHAPTER I

INTRODUCTION

1.1 SCOPE OF THE THESIS

Wireless Sensor Networking (WSN) is an important technology which continues to attract much research to bring about many benefits. This technology can be used in many applications, such as in military [1-2], engineering [3-4], agriculture [5-6], health [7], environmental [8], habitat [9] and volcano monitoring [10]. Also, dedicated systems have been developed for industrial applications [11-12], intelligent transportation systems [13], sport monitoring [14] and film production [15].

Practical WSN implementations are not just for deploying in the most populated urban areas [8], but also in isolated rural areas. Bird habitat monitoring [9], landslide early warning [16], and weather monitoring in wildland fire environments [17] are several examples of WSN applications in rural areas. Compared to WSN in urban areas, the development of WSNs in isolated areas poses many challenges. For example, such deployment often encounters harsh environment in isolated locations, and this could increase the difficulty and cost of WSN installation and maintenance. As such, the system cannot be attended as often as WSN in an urban area. Another challenge is the absence of public telecommunication infrastructure which may be used to interconnect sensor nodes (SNs) to a remote control station (CS) as is often the case normally for WSN in urban locations. As such, a dedicated long-distance communication link would need to be established to carry various data collected from SNs distributed in rural areas to the CS located in an urban area which could be hundreds of kilometres away. An alternative solution is the use of satellite communication to act as the backbone link as described in [9, 16, 17]. Often, the deployment of WSN in rural areas also encounters the lack of main power infrastructure. In such a situation, the operation of a WSN would have to rely on battery power. In order to extend the battery life, solar panels could be incorporated to act as an additional energy harvesting equipment [9, 16, 17]. Moreover, establishing a proper radio communication in the hostile environment also poses significant challenge due to the presence of various obstructions, including hilly terrains, dense vegetation, and also dynamic weather change that could significantly affect the radio signals quality. This thesis describes the study of an environmental WSN that has to overcome most if not all the above factors. The following paragraphs give an introduction to such a proposed system.

In this thesis, the WSN is purposed as an early warning system for people living in the Province of East Kalimantan, Indonesia from environmental disasters, such as flash flood, land slide, and forest fire. These disasters frequently occur in many areas of the province since people exploit natural resources by carrying out wood loggings, gold and coal mining, and establishing huge palm plantations. Flash flooding tends to occur on areas close to Mahakam River, including villages, towns, and even the capital city itself. As the length of the river is more than 900 kilometres, the flood has impacted an area of more than 900 square kilometres. On the other hand, landslides happen in areas that have high slopes. In the past, it has caused severely damaged villages and land transportations. Meanwhile, forest fires often occur in many areas far from the river where the forest has been cleared for oil palm plantations. Because of the lack of early warning, people living in these disaster prompt areas usually have to suffer from casualties and financial losses in the event of a disaster. It is envisaged that a wide area early warning system, as proposed in this thesis, could help to reduce or even prevent such losses.

There are hundreds of potentially disaster susceptible locations spread sparsely within this province. These locations are generally separated from one another by a long distance, possibly from kilometres to tens of kilometres away. Assuming that a cluster of sensor nodes (SNs) were to be deployed in each of these locations, the main challenge would be to find a way to effectively collect the data from these individual clusters of SNs to forward to the distant control station (CS) located in the capital city. A more straightforward approach would be the use of satellite links to connect the individual SN clusters with the CS. However, the costs of installing base stations plus ongoing subscription fees for a large number of SN clusters may prove to be too expensive. The alternative is to search for a more cost effective solution. It is the objective of this thesis to examine the use of a well-established radio technology, such as 802.11 standard [18] in conjunction with an appropriate network architecture to form a dedicated wide area WSN that could support a large number of widely distributed SN clusters. It is envisaged that nodes equipped with different transmit power levels would have to be introduced to cope with different network functions in a diverse range of propagation environments. For this reason, a multi-tier network architecture is proposed to accommodate nodes of different network functions. The proposed network architecture of the dedicated WSN infrastructure is shown in Figure 1-1.

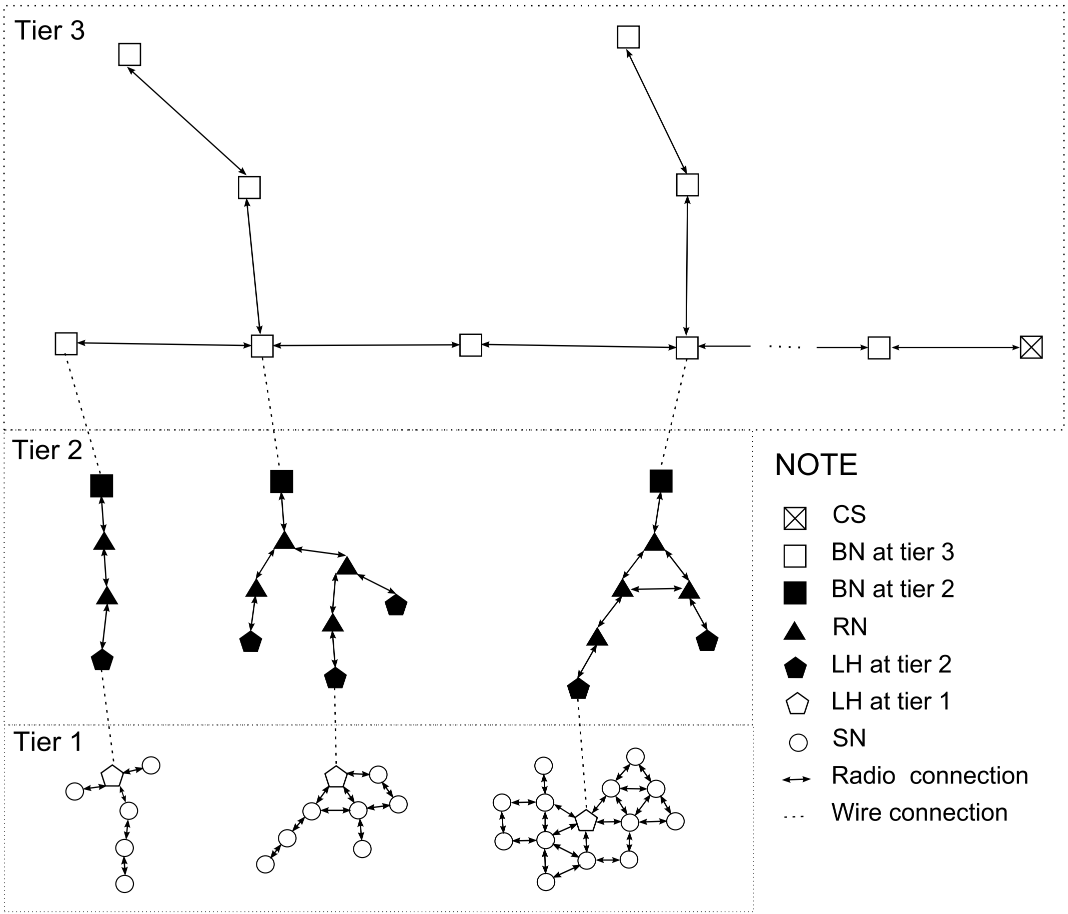

Figure 1-1 A proposed three-tier wide area WSN for environmental monitoring.

As shown in Figure 1-1, the proposed WSN is made up of three different layers, namely Tier 1, Tier 2, and Tier 3, operating with five types of nodes, which are SN, local head (LH), relay node (RN), backbone node (BN), and CS. The lowest network layer, Tier 1, is made up of a number of data collecting SNs distributed in a disaster prone area. These SNs are usually compact in size and battery operated so that they could be readily deployed [19 - 21]. In an attempt to conserve battery power, each of these SNs is equipped with a low power transmitter. As such its transmission range is limited to less than a kilometre, especially in a high propagation loss environment like forest with high dense vegetation and rough elevations. The topology of Tier 1 could be either tree or mesh depending on how individual SNs are being deployed. All SNs in a cluster will send their data packets to an LH, which acts as the interface between Tier 1 and Tier 2. If the distance between an SN and its LH is beyond its transmission range, then its data packets would have to be delivered to the LH via multihop transmissions through one or more intermediate SNs. Unlike a SN, a LH node is equipped with a higher transmit power to cover the longer transmission range to reach a BN or RN.

Tier 3 forms the main communication backbone of the proposed wide area WSN to deliver data packets collected from the various SN clusters to the remotely located CS. It comprises of a chain of BNs, each equipped with a high power transmitter to provide long distance transmission in excess of 50 kilometres between two adjacent BNs. Normally, the antenna for a BN is deployed on a tall tower on a high ground and above surrounding trees to minimize propagation loss. Also, the location of a BN has to be chosen in a not disaster prone area. Furthermore, solar panels are used to recharge the battery powering the high power transmitter.

Often, an SN cluster together with its LH could be located at a distance far beyond the single-hop transmission range between the LH and a BN. In this situation, one or more relay nodes (RNs) could be introduced to transfer data from the LH to the BN. This relay function is the responsibility of a Tier 2 link in the proposed wide area WSN. It is also possible to make use of a single Tier 2 link to connect not one but several SN clusters to a particular BN. Now, having Tier 2 relay links connected to various individual BNs, the topology of Tier 3 of the proposed wide area WSN then take on the familiar tree structure.

From the previous paragraphs, it is noted that the proposed WSN, under most instances, relies on multihop transmissions in all its three network layers. Such a network architecture makes it rather flexible to establish communications links between widely dispersed locations in normally harsh environments. Moreover, several studies in [22-24] show that multihop network involving the use of a carrier sense multiple access (CSMA) scheme, as in 802.11 radio, tends to suffer from performance degradation. One reason is possible packet collision due to the hidden node problem as studied in [25]. The so called exposed node in association with hidden node, is another likely factor in degrading the performance of a multihop network operating with a CSMA protocol. In this latter case, a node within the transmission range of a neighbouring node cannot transmit while its neighbour is transmitting [25]. Several methods have been proposed to enhance the performance of a multihop network by reducing the effect of hidden and exposed node problems as investigated in [26]. Among them, multichannel schemes have attracted a lot of attention since they make it possible for nodes to carry out some forms of simultaneous transmissions within the same coverage area [27-28].

With the use of multiple channels, it is necessary to adopt a proper channel assignment scheme for adjacent nodes to establish communication. These channel assignment schemes can be classified as fixed, semi-dynamic, and dynamic assignment [28]. Due to the varied forest environments that could affect differently the quality of a communication link, dynamic channel assignment may provide a more flexible operation. The operation of a dynamic channel assignment will usually involve two stages, which are channel negotiation/rendezvous and data exchange [27]. Channel negotiation procedure is first undertaken by a pair of nodes intending to exchange data, and before the data is sent from the sender node to the destination node. Depending on how channel negotiation is carried out, dynamic channel assignment can be further classified into dedicated control channel, split phase, and frequency hopping. A dedicated control channel scheme [29] assigns a specific channel for the rendezvous, and other remaining channels for actual data exchanges. By relying on only a single channel for negotiation, a bottle neck could occur when a significant number of nodes are also contending for the control channel to perform negotiation. On the other hand, the operation of split phase [30] and frequency hopping [31] will rely on the use of time slots that requires time synchronization provided by a central control. In view of this, such channel assignment schemes are not suitable for the wide area WSN studied in this thesis. Instead, a multichannel scheme using a different approach will be introduced for the long chain multihop operation of Tier 3 and Tier 2 of the proposed WSN. As the hidden and exposed node problems occur within a 2 hops distance, it is the aim of the study to make use of as small a number of frequency channels as possible, operating in conjunction with spatial frequency reuse, to achieve the required network performance. Such practice is also required for efficient spectral utilization as well as equipment cost consideration.

Nowadays, the performance of a given WSN is often evaluated using a computer simulation package, such as NS3 [32]. Moreover, a simple method for throughput estimation could help in quickly gaining valuable insight into the influence of any changes made to the network architecture. Several methods on network capacity estimation have been published in [33-35]. These methods assume that a network has a number of nodes deployed in a given area but with no consideration to the actual network topology. Such methods may either overestimate or under estimate the capacity for a given specified network configuration [36]. In [36-38], modifications have been made to the methods previously proposed in [33, 35] by taking the network topology into consideration. The topologies considered are spanning tree [36], and grid and ring [37] Nevertheless, such methods involve a significant amount computations and complex topology formulation particularly for network with irregular configurations. On the other hand, a simple capacity estimation method that can deliver a quick result could be beneficial for use in the field where changes to the network are routinely taking place. One such capacity estimation method, that can be readily applied to Tier 2 and Tier 3 of the proposed WSN, is presented in Chapter 4.

Moreover, another concern to the study of WSN in this thesis is the performance of the network in handling two-way traffic. In this thesis, forward traffic refers to those data packets travelling from SNs towards the CS, while those packets coming from CS and end up at the various SNs are called reverse traffic. Normally, reverse traffic carrying command and control messages for network supervision and management is given preference for delivery to the intended destinations. Forward traffic, on the other hand, could succumb to access the channel when both traffic types are present, as data messages contained in the forward traffic are frequently updated. It can deliver data messages frequently. For this reason, priority is to be given to the reverse traffic over the forward traffic in accessing channel resource.

One way to ensure preference of deliveries of reverse traffic is to make use of the priority feature built into 802.11e protocol [39]. In this thesis, the protocol assigns short interframe space (IFS) and small contention windows (CW) size to command packets with higher priority while lower priority data packets, which are normally larger in size, are assigned a long IFS and large CW size. As a result, the normally smaller but higher priority packets can have a quicker access to channel resource. However, it is observed that when the data rate of the reverse traffic is much lower than that of the forward traffic, the network tends to be overwhelmed by the forward traffic. Thus, the reverse traffic is left with only a very short time space for accessing the channel resource. Therefore, it becomes necessary to find another scheme that will provide a better priority for reverse traffic to access channel resource. This will be further discussed in Chapter 5.

1.2 OBJECTIVES AND CONTRIBUTIONS

In addressing the wide area WSN proposed for deploying in a sparsely populated rural area, a number of issues have been identified which require further consideration. These are:

a. Enhancement of the performance of wireless multi-hop transmission, such as network throughput, in Tier 3 and Tier 2 of the proposed WSN. The research will focus on minimizing the effects of the so called hidden node and exposed node problems associated with a multi-hop network operating with a CSMA protocol. This involves the use of multichannel medium access control (MAC). This MAC uses a distributed control and a small number of frequency channels.

b. Derivation of a simple but sufficiently accurate method for a quick network performance estimation. Such an estimation method is crucial for field use in predicting network performance whenever changes are made to Tier 3 and Tier 2 of the proposed WSN.

c. Investigation into the use of a priority support scheme that could improve packet deliveries for the reverse traffic in two-way communications. This is particularly important for the operation of Tier 3 of the proposed WSN that has to handle the various time sensitive messages, such as supervisory and control messages, originated from the CS to its intended SNs.

During this study, several original contributions have been made. These are:

a. A multichannel MAC protocol, addressed in Chapter 3, is proposed for enhancing the throughput of long chain multihop networks found in Tier 3 and Tier 2 of the wide area WSN studied in this thesis. With this MAC, a node located two hops away from a current transmitting node will use a transmission channel, which is not the same as that used by the transmitting node, for its transmission provided that channel is idle. This particular channel is determined by the intermediate node locates between these two nodes. The final choice of this channel is made by the intermediate node after its consideration of the actual channel used by the transmitting node as well as the channel used by itself. After that, the information of the preferred channel will be delivered to the concerned node by either piggybacking the message in a reserved bit of 802.11 MAC header, or added on to the payload if the information is more than one bit. Doing it this way will reduce the communication overhead. This proposed MAC protocol will be referred to in this thesis as 2-hop channel reservation (2HCR).

b. A simple method for predicting network throughput associated with Tier 3 and Tier 2 of the proposed wide area WSN is described in Chapter 4. It is based on the observation that any network architecture of Tier 3 and Tier 2 can be decomposed into a set of basic topologies. The throughput achievable with each of these basic network topologies is determined through computer simulations for a particular MAC under consideration. For example, the throughput of a target network can be estimated by decomposing the network in an iterative manner until the final network matches one of the above known basic network topologies. In the way, the estimated throughput of the target network is the same as that particular basic network topology. It is found that the difference in throughputs obtained by computer simulation and using the proposed estimation for a number of different network architectures is less than 10 %. This observation holds true for the three CSMA schemes considered: 2HCR, MC CSMA, and 802.11b.

c. In Chapter 5, a priority support protocol is proposed for enhancing packet delivery of reverse traffic in bidirectional WSN. This protocol is particularly crucial in an asymmetric situation where the data rate of reverse traffic is very low compared to the data rate of forward traffic. In this situation, forward traffic packets are flooding the network and leaving a short time space for reverse traffic to access the network. As a result, the packet delivery rate of reverse traffic is lower than that of forward traffic. The protocol 802.11e [39] has been proposed for correcting this situation by assigning the reverse traffic a shorter interframe and contention window. However, simulation result shows that this protocol provides small improvement on reverse traffic packet delivery rate. For asymmetric situation, packet delivery rate of reverse traffic is still below the packet delivery rate of forward traffic. This is because reverse traffic has less opportunity compared to forward traffic in accessing the channel resource due to the domination of high data rate forward traffic. To overcome this shortcoming, another strategy to improve reverse traffic packet delivery is by suppressing forward traffic throughput. To achieve this, RTS/CTS messages are applied to reverse traffic. These messages are exchanged prior a reverse traffic packet transmission. Upon overhearing the messages, neighbouring nodes of both reverse traffic packet sender and destination will stop transmission in anticipation of a reverse traffic packet to be delivered. As a result, the throughput of high data rate forward traffic reduces significantly, and thus giving more opportunity for reverse traffic to access the channel. Simulation results show that this scheme could derive a better reverse traffic performance than that provided by 802.11e scheme. Nevertheless, for asymmetric situation, the packet delivery rate of reverse traffic is only slightly below the packet delivery of forward traffic. This is possibly because reverse traffic still faces a significant channel contention with the suppressed forward traffic. Despite 802.11e and RTS/CTS priority schemes could not derive reverse traffic packet delivery higher than forward traffic packet delivery, each of them has a mechanism that is useful to provide a priority support as shown by their individual simulation result. Such useful mechanisms then are harnessed by a proposed priority support scheme so called a simple priority support. In this scheme, the ability of RTS/CTS in suppressing forward traffic is combined with IFS diversity in 802.11e to provide a better priority support. Simulation result shows that in asymmetric situation, simple priority support scheme could derive reverse traffic packet delivery rate that is higher than forward traffic packet delivery rate.

1.3 STRUCTURE OF THE THESIS

Chapter 2 firstly addresses WSN architectures including single tier and multitier networks. This is then followed by a discussion of advantages and disadvantages associated with these two network types. It is noted that one disadvantage of multihop network is throughput degradation caused by the so called hidden and exposed node problems when a CSMA scheme is adopted. A review of several methods, published in the literature, for minimizing the effects of hidden and exposed nodes in multihop networks is presented. Among them, an approach that utilizes a multichannel MAC is further studied. This type of MAC makes use of multiple channels to enable simultaneous transmissions by multiple nodes to improve multihop network throughput.

In Chapter 3, a multichannel MAC called 2-hop channel reservation (2HCR) is purposed to improve the performance of multi-hop networks, particularly in the form of a chain topology. The mechanism of this MAC is presented in Section 3.3. To evaluate the performance of 2HCR in comparison with the performance of 802.11b [18] and MC CSMA [40] protocols, a computer simulation procedure is described in Section 3.4, with the relevant results presented and discussed in Section 3.5.

Furthermore, an estimation method for predicting the throughput of a rather complex network is described in Chapter 4. The discussion on the estimation procedure begins with an explanation of the basic topologies and their associated throughputs. Then an example is provided to show the iterative procedure for decomposing a relatively complex network to be finally represented by one of the simple topologies in the basic network topologies set. A number of comparisons between the estimated and computer simulated results are undertaken to evaluate the accuracy of the proposed estimation method. These comparisons include the use of three CSMA schemes, namely 802.11b, MC CSMA and 2HCR protocols.

While Chapter 3 examines the performance of the proposed 2HCR compared with the performance of 802.11b and MC CSMA in a unidirectional network, Chapter 5 evaluates the performance of the three protocols in bidirectional network where both reverse and forward traffics are present. In Section 5.2 of Chapter 5, it is addressed the performance of 2HCR in bidirectional traffic in comparison with 802.11b and MC CSMA. As it is desired to have packet delivery of reverse traffic higher than packet delivery of forward traffic, Section 5.3 investigates the implementation of 802.11e QoS protocol to provide a priority support for reverse traffic. Meanwhile, Section 5.4 addressed another strategy to provide a priority support by using RTS/CTS scheme. As the priority support schemes in Section 5.3 and Section 5.4 have not provide reverse traffic packet delivery higher than forward traffic packet delivery, a simple priority support is proposed in 5.5.

Finally, Chapter 6 draws conclusions and makes several recommendations for future study of WSNs in rural areas.

CHAPTER 2

LITERATURE REVIEW

2.1 INTRODUCTION

While some wireless sensor networking systems are targeted for deployment in populated metropolitan areas around cities or suburbs [8], several studies have proposed wireless sensor networks (WSNs) specifically designed to be installed in rural villages [9, 16] and unpopulated region [17]. Unlike WSNs located in cities and towns, it becomes very challenging to deploy WSNs in remote rural regions, which lack both electrical mains power supply and readily accessible telecommunications infrastructures. These two constraints play a crucial role in determining the type of network architecture appropriate for a WSN to be feasibly deployed in a rural region.

Sensor nodes (SNs) in a rural WSN are generally powered by battery. Recently, new technologies of power harvesting, such as from solar cells, could be introduced to extend the operating lifetime of SNs, thus further support the development of WSN in remote regions. Often, mainstream telecommunication services do not exist in remote under-populated regions. As such, satellite communication could be the only viable or available means for the delivery of remotely collected data by the SNs to the central control station (CS), normally located in the metropolitan, for further processing. However, satellite communication links tend to be too expensive for many applications, particularly for those rural WSNs that are required to continuously monitor multiple locations widely spread over large distances. For such applications to remain feasible, it may be necessary to develop a more cost-effective solution for the delivery of data between the various remotely distributed SNs and the CS. This is the main driving force behind the research presented in this thesis.

Furthermore, it has been common to evaluate the performance of WSN using a computer simulation. By using this method, various network capacity estimations such as in [33-35] have been published. These estimation methods will be examined in Section 2.5 to look at their capabilities in predicting irregular network configurations in Tier 2 and Tier 3 of the architecture described in Section 1.1 of Chapter 1.

Moreover, due to the hostile environment of rural area where SNs are deployed, large number of SNs locations, and long distance between CS and SNs, it will give a benefit if CS can provide remote network supervisory and management. With this function, time consumption and cost of in-site attendance could be reduced significantly. The implementation of remote network supervisory introduces an additional control traffic that flows in opposite direction of the existing data traffic. While the data traffic flows from SNs to CS, the control traffic flows from CS to SNs or other nodes in the network. In the presence of both traffics, the control traffic may not be successfully delivered to the destination, particularly if the data rate of control traffic is very lower than the data rate of data traffic. Due to the important role of control traffic in supporting a successful network management, a high priority in accessing the network must be given to this traffic. Several methods to support priority for the control traffic are addressed in Section 2.6.

2.2 WIRELESS SENSOR NETWORK ARCHITECTURE

2.2.1 Basic Wireless Sensor Network Architecture

In general, a basic WSN is made up of multiple sensor nodes distributed within a given sensing field, as shown in Figure 2-1. The data collected by individual SNs is passed on to the sink for further processing. For applications involving a local area, the sink is also the destination for the WSN. However, in the case of the final destination being located at a greater distance away from the sensing field, the data accumulated at the sink node will then have to be relayed to CS using either public telecommunication services, such as GPRS [41, 42], UMTS [43], ADSL [44], and CDMA [44], or satellite links [9, 16, 17]

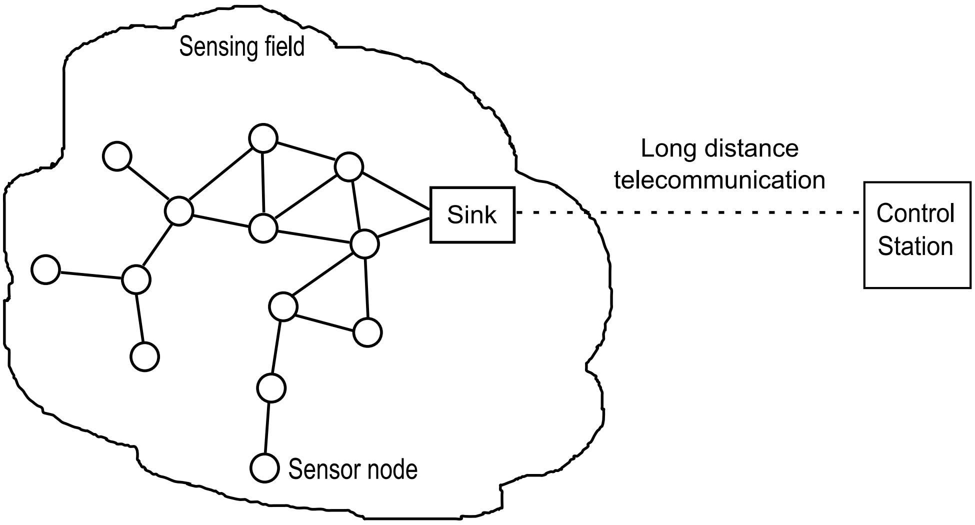

Figure 2-1 A basic wireless sensor network architecture

An SN unit normally consists of four basic functional elements, and these are sensing, processing, transceiver, and power supply units [45], as illustrated in Figure 2-2. The main part of the sensing unit is often in the form of an analogue transducer, which translates the surrounding phenomenon into an analogue electric signal. The processing unit then converts the analogue signal into a digital form by means of an analogue to digital converter. The resulting data is then assembled together with other information, such as sender and destination addresses, time stamp, and any other communication protocol requirements, into an appropriate data packet for onward transmission by the transmitter in the transceiver unit.

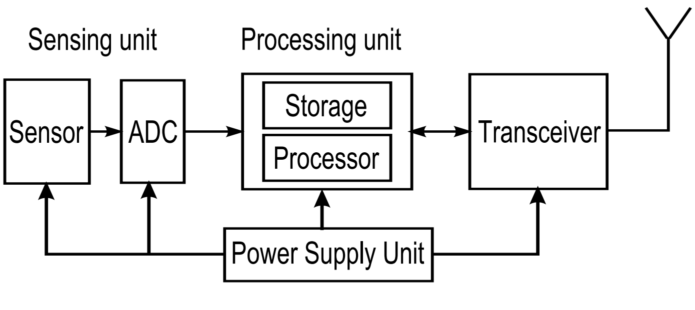

Figure 2-2 The elements of a sensor node (SN)

As WSN is intended to work with a large number of SNs, this means that the cost of a single SN could have a great impact on the economic feasibility for a given application. For this reason, the cost of an SN is intentionally kept low by adopting as far as possible low cost and low power electronics, such as micro-electromechanical (MEM) transducers, microcontroller, and single-chip transceiver. Short-range radio communication is often chosen to conserve power supply, which for most WSN applications, is derived from battery.

Also, deploying and maintaining a WSN operating in some remote hostile environments could be expensive and possibly dangerous. Therefore, it is desirable to be able to leave the SNs, after the initial installation, to operate on their own for long period of time, often for months and even years. One way to achieve this is to include in the WSN design techniques, such as network self-organization [46], routing [47], data gathering [48], and sleep scheduling [49] for efficient network deployment and power management [50]. Nowadays, the lifetime of batteries used in WSN can also benefit from the recent development in power harvesting technology. Besides the popular use of solar cells for recharging batteries, it has been shown that electrical power could also be readily derived from the surrounding environment in the form of wind [51], heat [52], and even water flow in river [53]. These sources could be exploited to enhance the power supply reliability in WSN.

2.2.2 Multitier Wireless Sensor Network Architecture

A WSN that is deployed to monitor a small sensing area usually consists of a number of SNs with a local sink in a single tier network architecture, as shown in Figure 2-1. This simple architecture is generally used in many applications, such as bridge structure [3], volcano activity [10], and industrial [11] monitoring. However, if the monitoring coverage area becomes so large, that groups of SNs have to be dispersed in different locations beyond the normal communication range of a SN, then it may be desirable to consider a multitier network architecture to link the various groups of SN together.

Unlike a simple single tier network that normally comprises of SNs with homogeneous functions, nodes in different tiers of a multitier network may be called upon to perform functions specific to a given tier [54]. To provide a specific function to each tier, the hardware of node in every tier could be physically heterogeneous or homogeneous. Next paragraphs describe several situations where multitier WSN comprise either heterogeneous or homogeneous nodes.

An example of multitier network with homogeneous nodes is described in [55]. In this network, a very large number of SNs deployed in a given sensing area are to be divided into smaller groups or clusters of SNs. Each cluster of SNs is coordinated by a cluster head (CH), which is chosen from among the cluster members during the cluster formation process. Often, a cluster is formed based on certain considerations, such as energy efficient [56], fault tolerance [57], or how many neighbouring nodes are transmitting "hello" messages during cluster initialization in a specified time defined by timer [58]. Generally, the choice of a CH is decided based upon the energy level of individual cluster members, with the CH assumes to consume more energy than the other cluster SNs. The higher energy consumption is needed by the CH to undertake activities such as aggregating data collected from the cluster members as well as performing inter cluster communication.

Once the clustering process has been completed, the two tiers architecture is performed, with the lower tier provides communication between individual cluster members and the CH, while the upper layer is responsible for communications among the various CHs and the eventual destination node. Therefore, during network operation, SNs in a cluster will sense and collect the environmental physical data and forward them to their CH. The data is then aggregated by the CH in preparation for onward to the sink. This two-tier operation has advantages when compared to a single tier sensor network, as explained in the following paragraphs.

In a single tier network, data packets of individual SNs are delivered to the destination node most likely by means of multihop communication. If the network size is very large with hundreds or even thousands of SNs, then it is possible that a high data traffic could be generated within any part of the network. When this occurs, it could give rise to traffic congestion in the network leading to an increase in transmission delay and possible packet drops. Furthermore, as intermediate nodes are likely to be called upon to forward a large number of packets, this could result in an inefficient use of energy in the network.

On the other hand, in a two-tier network with multiple clusters of SNs, SNs within a cluster only need to forward data packets to its local CH, which is generally located at just one or a few hops away. As a result, the volume of traffic flowing within the entire network is reduced. In this case, the likelihood of traffic congestion caused by unnecessary high packet retransmissions is also reduced. With this decrease in traffic volume and subsequent packet retransmissions, the total energy usage of the network could also be reduced to prolong the battery life of the network.

Although multitier network with homogeneous nodes has given advantages as discussed above, in some cases, CH needs to be equipped with more powerful computation, transceiver, and power supply units. This enhancement is required if CS must provide extended data processing or/and long-distance transmission that cannot be derived by the existing homogeneous nodes. For example, the network described in [59] employs a CH to act as a gateway node that performs data aggregation and long-distance transmission to CS. Hence the CH is equipped with enhanced processing unit, high power transceiver and power supply.

For a rural area WSN where SNs clusters are deployed sparsely, and the distance between clusters and CS is too far, a multitier WSN with heterogeneous nodes will be useful to be implemented, as shown by research in [9,17]. In [9], an environmental habitat monitoring WSN has been deployed in Great Duck Island to observe the disturbance effect of-human presence to the behaviours of seabirds in the area. The system employs a two- tier architecture, made up of the so called patch network and transit network. The latter is used to connect the various network patches, set up in different locations, to a field unattended base station (BS).

In this particular WSN, the lower tier patch network is configured with several low-power consuming SNs and a gateway. Each SN, powered by batteries, is responsible for the tasks of sensing the environment and collecting the relevant data, simple data processing, and intra-patch networking. The gateway node, on the other hand, is configured with 2.5 W Strong-arm embedded system, a 916 MHz transceiver, and a 14 dBi directional Yagi antenna to provide the required computational capabilities for data aggregating and longer range wireless communication. The electrical power of a gateway node is derived from a combination of rechargeable batteries and solar panel. Several such patch networks with their respective gateway nodes then form the transit network for the delivery of the aggregated data, collected by SNs at various patch networks, to the BS. The communication between each gateway node and the BS is carried out by a single-hop radio link.

Another WSN, called FireWxNet [17], has been established for monitoring forest fire. It has also adopted a two tier architecture. As well as in [9], this WSN the lower tier comprises of low cost SNs, while the upper tier consists base station (BS) nodes equipped with more powerful computation and transceiver unit. The main difference between this WSN and the one described in [9] is that the upper tier of this network is designed to make use of multihop transmission to cover the long distance between two adjacent BS nodes. A diagram of the FireWxNet WSN is shown in Figure 2-3. SNs in the lower tier have a transmission range of up to 400 metres. These SNs are used to collect weather information, including wind speed and direction, air temperature, and humidity from the environment. The collected data by individual SNs is then delivered to a local BS to be aggregated before forwarding to the Incident Control station located almost 100 km away by means of multihop links. As the data collected by Incident Control Station need to be accessed by Weather Management Information System office separated hundreds kilometres away, FireWxNet enables long range communication via satellite links. In the field, FireWxNet is only deployed on a specific location between two to eight weeks, and then it is moved to another location.

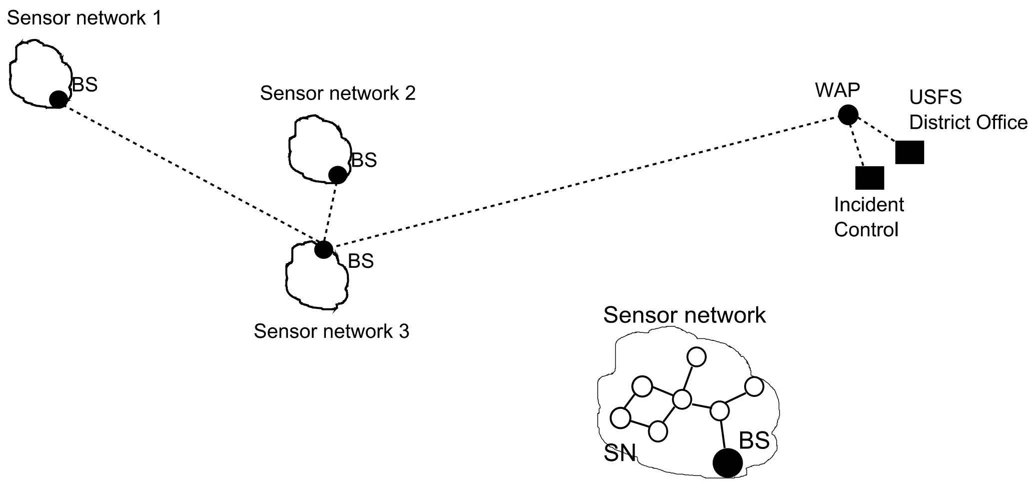

Figure 2-3 A diagram of FireWxNet in Bitterfoot National Forest Idaho, USA.

Since situation encountered by the environmental WSN studied in this thesis may be similar with the situation on FireWxNet deployment area, the study may refer to FireWxNet system. However, more challenges are encountered by the environmental WSN due to situations explained below. First, number of SNs cluster in FireWxNet is only three, while number of SNs cluster in environmental is much more larger. Hence, network configuration of environmental WSN is more complicated than that illustrated in Figure 2-3. Second, the observation area of FireWxNet consists of pine forests in the valley, and clear area at the peak of the mountain. Thus, communication between BSs can be established by long distance and line of sight (LoS) links with a few hops. On the other hand, rural area where the environmental WSN will be deployed, consists of dense tropical forest on the mountainous areas. Establishing long range and LoS links may be too difficult due to the presence of high trees and dense vegetation than can increase the propagation loss. Therefore, long chain multihop networks would be more suitable. Third, as the distance between SNs cluster to other SNs clusters, and between SN clusters to CS is far and could be up to hundreds kilometres, the use of long chain multihop network is more obvious. Finally, as FireWxNet is operated for only several weeks, a concern on power consumption may not be as high as in environmental WSN that is intended to be operated in a longer period.

2.3 WIRELESS MULTIHOP NETWORK AND ASSOCIATED THROUGHPUT DEGRADATION

In Section 2.2, it is shown that data packets are almost always delivered from source to destination via multihop communication links, irrespective whether the network architecture is single or multiple tiered. For example, in the case of FireWxNet, depicted in Figure 2-3, as well as in environmental WSN explained in Section 1.1 of Chapter 1, the multihop transmission between nodes is carried out without the need for centralized network control, i.e., the coordination between nodes is done in a distributed manner.

Now, consider the use of the distributed coordination function (DCF) available in the very popular 802.11 standard [18] as the protocol for implementing multihop communication in a multihop WSN. This DCF protocol has been widely studied in applications described in [22-24]. It is reported in [22-24] that the throughput of a multihop WSN achieved through the use of DCF, decreases when the number of hops is increased. Significant factors affecting such throughput degradation are hidden and exposed node problems as explained in the following paragraphs.

Study in [25] addresses the effect of hidden and exposed nodes problems to the network capacity. When such situations occur, data packets may be dropped or subjected to longer delivery time with the consequent reduction in network throughput. Now, assume uniform transmission range between each pair of adjacent nodes, a hidden node scenario is illustrated as in Figure 2-4. In this case, node N3, being two hops away, cannot hear the transmission of N1, and vice versa. Similarly, N4 cannot hear the transmission of N2, and vice versa. Therefore, N1 and N3 form a hidden node pair, while N2 and N4 become another hidden node pair. Under this situation, if N3 sends a packet to N4 at the same time when N1 is sending a packet to N2, a collision will occur at N2. Moreover, N1 could recognise this collision when it fails to receive an acknowledgement from N2 during the predetermined waiting period. As such, N1 may back-off before it retransmits the packet.

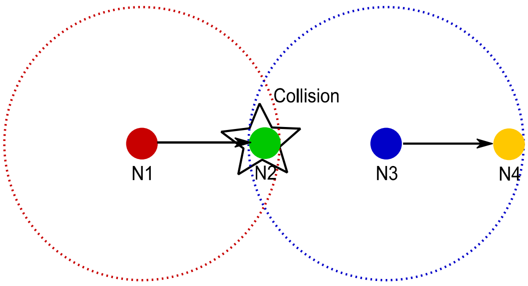

Figure 2-4 A hidden node scenario with the transmission range of a given node denoted by the dotted circle radius.

An exposed node scenario in a multihop network is shown in Figure 2-5. Under this situation, N3 should be allowed to send its data packet to N4 while N2 is delivering its packet to N1, as N1 and N4 should receive their respective data without no possibility of collision. However, if N2 transmits earlier than N3, N3 recognizes that the channel is busy. Consequently, N3 will hold back its transmission, and wait until the channel becomes idle.

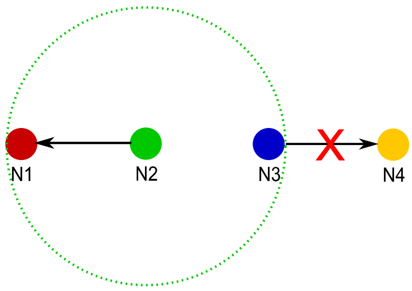

Figure 2-5 An exposed node scenario

Yet, it is also possible for an exposed node problem to occur when RTS/CTS handshaking is adopted, as depicted in Figure 2-6. In this case, N1 wishes to forward data to N2, while N4 intends to send data to N3. Such simultaneous transmissions could take place without collision as the transmission range of N1 does not reach N3. Similarly, the transmission range of N4 is short of reaching N2. To begin a data delivery process, N1 first sends an RTS message, RTS1, to N2, and N4 also sends an RTS message, RTS2, to N3. Now, if RTS1 is sent earlier than RTS2, as shown in Figure 2-6, then N2 in response will send a CTS message, CTS1 to N1 earlier than N3 sending CTS2 to N4. As N3 is within the transmission range of N2, it would also receive CTS1, and thus hold back its transmission by network allocation vector (NAV) period. Consequently, N4 would have to delay sending its data to N3.

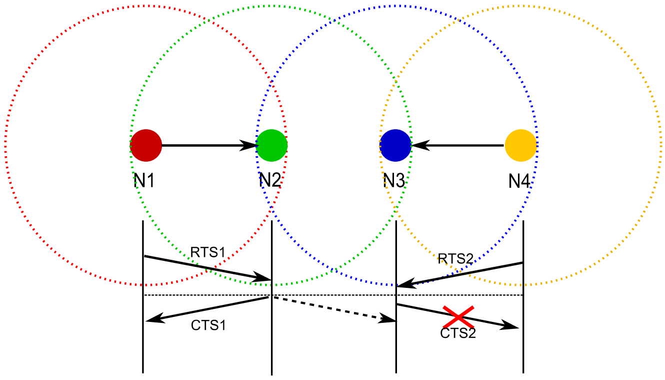

Figure 2-6 An exposed node problem caused by RTS/CTS handshake.

The above observations are usually associated with multihop wireless network. This research will however focus on how to overcome throughput degradation, caused by hidden and exposed node problems, that particularly occurs at long chain and irregular tree topologies in Tier 2 and Tier 3 of the network architecture depicted in Figure 1-1. Several works in this area including in [22-24] have investigated a single source chain topology with up to ten hops. It has been shown by means of computer simulations that the throughput of a chain network decreases as the number of hops is increased [22-23]. Their results followed the relationship given in [60], i.e., the normalized throughput is inversely proportional to the number of hops. This relationship has also been verified by an experiment carried on a 5-hop wireless network. The above relationship between throughput and hop number is valid only when an input data rate would give rise to the highest throughput in a chain network with about ten hops, is used.

2.4 ENHANCING THE THROUGHPUT OF WIRELESS MULTIHOP NETWORK

Throughput of a wireless multihop network could be improved through the use of an effective multiple access control (MAC) protocol, which plays a crucial role in delivering data packets. Very often, this is done in conjunction with the PHY layer through cross layer modification. Also, a number of schemes have been devised to overcome somewhat the effect of hidden node problem. Such schemes are normally classified into pure contention based, busy tone based, directional antenna based, and multiple channel based [26].

Protocols based on pure contention have been studied in [61-63] as they usually do not require modification to the hardware based on the standard 802.11 communication protocol. The mechanisms of these protocols are commonly based on CSMA-CA, where channel sensing is undertaken first, then followed by the exchange of control messages in an attempt to avoid collision due to hidden node problem. The control message may be initiated by either the sender, the receiver, or both parties (i.e., hybrid).

The four-way handshake mechanism specified in 802.11 protocol [18], involving RTS, CTS, DATA, and ACK control messages, is an example of sender initiation (SI). With this protocol, when a sender wishes to deliver a data packet to a receiver, it first sends an RTS message to enquire the receiver. This RTS message is transmitted by means of broadcast, so that other nodes located within the sender transmission range will withhold from transmission for an RTS NAV period. Meanwhile, upon receiving the RTS message, the receiver would answer the enquiry by broadcasting a CTS message. This CTS control message is translated by other neighbour nodes located within the transmission range of the receiver, as a command to hold back their transmission for a CTS NAV period. Furthermore, upon receiving the CTS message, the intended sender will start to transmit the DATA packet to the receiver. Upon receiving the DATA packet, an ACK message would be send by the receiver to inform the sender that the DATA packet has been successfully received, thus ending the four-way handshake.

On the other hand, the exchange of control messages can also be initiated by a receiver, i.e., receiver initiation or RI, as described in the multiple access with collision avoidance by invitation (MACA-BI) protocol [62]. In this case, when a node is ready to receive a data packet, it broadcasts a ready to receive (RTR) message to the sender. With the exception of the intended sender, all other nodes within the proximity of the receiver will withhold transmission for a defined period, which is calculated from the information of packet size contained in the RTR message. Upon receiving this message, the sender will then forward the DATA packet to the receiver without the worry of packet collision caused by transmissions from other neighbouring nodes.

Proper operation of an RI protocol, however, would require that the potential receiver is able to recognize the transmission schedule of the potential sender. This is done by having the receiver to manage the polling of its neighbouring nodes and the traffic prediction algorithm, which operates based on the information of the frame queue length and data arrival rate piggy-backed on the DATA packet sent by the potential sender.

As an RI protocol, such as MACA-BI, operates with few control messages, the cost of communication overhead is therefore reduced. Consequently, this leads to more energy efficient transmission and shorter communication procedures. Furthermore, MACA-BI allows neighbouring nodes of a potential sender to keep on transmitting as collisions due to hidden node problem could only be caused by untimely transmissions of the neighbouring nodes of the receiver. On the other hand, MACA-BI can only work properly in a predictable traffic pattern environment.

The hybrid channel access scheme presented in [63] makes use of both SI and RI to take advantages of these two mechanisms. The author of [63] suggests that RI may give a better performance over SI in view that collisions only take place at the receiver. This is because the receiver has more knowledge of its surrounding environment than the sender, due to its polled data and the traffic prediction algorithm. However, such a hybrid protocol has not been widely accepted for use in ad-hoc networks due to its lack of ability to adapt to the constantly changing environments of an ad-hoc network. Normally, a hybrid protocol operates with SI set as the default mode, whilst RI is utilized only when the SI does not perform well. Both the determination of SI performance and the mode selection are carried out at the sender. In the event that an RTS message sent by a sender fails to receive a response from its intended receiver after a defined period, the sender would then forward an RI mode change message via any subsequent packets, to inform the intended receiver to change into RI mode. Upon receiving an CTS message from the intended receiver, the sender would switch to operating with the RI mode until its packet queue is empty.

As addressed above, pure contention methods rely on the existence of control packet to alleviate data packet collision affected by hidden node problems. The control packet commonly informs neighbour nodes of the sender and destination nodes to hold their transmission during packet delivery from the sender to the destination. However, this mechanism causes several drawbacks. First, the control packets may be too costly as a communication overhead, if the size of data packet is too small. In 802.11 standard [18], the use of control packets RTS and CTS is optional. It may be enabled if the size of data packet is sufficiently long, e.g. more than 2200 bytes, as the default in NS3 simulator [32]. Hence, if the size of data packet is too short, it may be better to consider another method for minimizing the effect of hidden node. Second, the presence of RTS/CTS for short size packet may significantly increase the collision probability rate as addressed in [64]. This is because RTS/CTS packets appear more frequent than RTS/CTS in long size packet transmission.

Meanwhile, the receiver initiated busy tone multiple access (RI-BTMA) scheme, described in [65], is an example of a busy tone protocol. It makes use of a data channel and a separate control channel, which are divided into individual time slots. These time slots also serve to provide the necessary synchronisation for transmissions by individual nodes.

Due to the absence of control message, a potential sender just sends its data packet to the receiver, using the data channel, once it senses that the control channel is idle. However, if it hears a busy tone, it performs the back off procedure until the control channel becomes idle. A data packet is made up of a one timeslot preamble field while the actual data field can occupy several time slots. Upon receiving the preamble field, an intended receiver will immediately transmit a busy-tone via the control channel acknowledging to the sender that the data packet is being received.

This process serves to inform its neighbouring nodes to hold back their transmissions until the end of the busy-tone, thus avoiding collision.

Another busy-tone protocol is the dual busy-tone multiple access (DBTMA) described in [66]. An objective of this protocol is to avoid node synchronization as used in RI-BTMA. Instead, DBTMA makes use of RTS and CTS messages exchanged via the control channel in the form of two distinct busy-tones, namely the receive busy-tone (B_{Tr}) and the transmit busy-tone (B_{Tt}). B_{Tr} is turned on by the target receiver upon receiving the RTS message from the sender, whilst the B_{Tt} is activated by the sender for a data transmission data period, after it has received a CET message from the receiver. This B_{Tr} tone also serves to alert other nodes in the vicinity of the receiver to hold back transmission until the end of the tone. In a similar manner, neighbouring nodes of the sender will withhold their transmission when they receive a B_{Tt} tone. The use of such procedures means that it is not necessary to include an acknowledgement message in DBTMA.

Busy-tone approaches require a separated channel to be used only for transmitting busy tone. It may be inefficient, particularly if the operation channel is limited. Despite the additional channel used only for busy tone, it could be better to use for data exchange, that may give significant enhancement to the network throughput.

The use of directional antennas is yet another way to enhance throughput in a WSN. This is achieved by means of spatial reuse to allow simultaneous transmissions on the same frequency by a number of nodes in given area. Figure 2-7 shows how the directional antenna radiation pattern can reduce the effects of hidden and exposed node problems. Figure 2-7 (a) illustrates that N1 and N3 intend to send their data to N2 and N4 respectively. A properly designed directional antenna normally has a very large gain in the desired direction with only weak side lobes. This means that the signal received at N2 from N1 is much larger than that from N3. As a result, the transmission of N3 is not likely to cause collision at N2, thus avoiding the hidden node problem. On the other hand, the transmission of N2, as shown in Figure 2-7 (b) is directed to N1 and away from N3. This suggests that the interference from N2 will be too small to prevent N3 from transmitting to its desired target at N4, thus minimizing the effect of the exposed node problem.

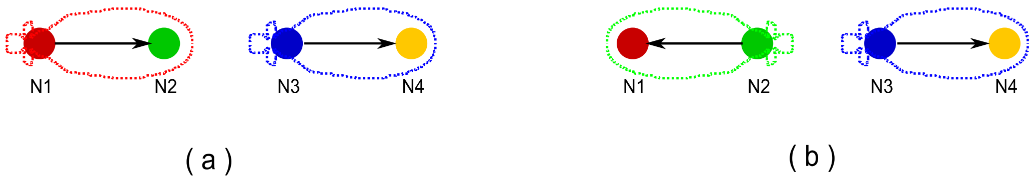

Figure 2-7 Examples of directional antenna radiation patterns aimed at reducing the effects of (a) hidden node, and (b) exposed node problems.

In an ad-hoc WSN, spatial reuse is achieved through the use of an adaptive antenna with its main beam in the direction of a target receiver. On the other hand, an omnidirectional antenna is used by a node to receive data as well as for sensing the status of the channel.

Directional MAC (DMAC) [67] is a protocol that incorporates the use of directional antenna in its operation. With DMAC, every node will first sense the channel status before it is allowed to transmit. Each node makes use of the individual transmissions from its neighbouring nodes to build up and store the direction information in the form of a directional network allocation vector (DNAV) table. If a node intends to deliver data packet, an RTS packet is transmitted with the antenna main beam pointing to the direction of its target receiver as indicated in DNAV. Upon receiving the RTS packet, the target receiver then replies with a CTS message packet in the direction of the sender. This is then followed with the transmissions of DATA and ACK to complete the current packet delivery. Finally, the information on the antenna direction and transmission duration is used to update the DNAV at both the sender and receiver for use in their next data packet delivery cycle.

With an RTS message being transmitted in a unidirectional manner in DMAC, it is possible that not all the neighbouring nodes of a sending node are able to receive this message. In the event that this RTS message has not been sent in the direction of the intended receiver, this gives rise to a so-called deafness problem.

The circular directional RTS MAC (CDR- MAC) protocol [68] has been proposed for overcoming this deafness problem. With this protocol, an RTS message is repeatedly transmitted by a potential sender aiming at several different directions, in an attempt that the intended receiver would be able to pick up one of these transmissions. Otherwise, CDR-MAC operates in a similar fashion as DMAC.

Yet another protocol has been proposed in [69] that utilizes an omnidirectional antenna for RTS/CTS transmission and directional antenna for DATA/ACK transmission. In this case, all the neighbouring nodes would now be able to receive the RTS/CTS message, thus avoiding the deafness problem. However, as shown in Figure 2-8 (a), an omnidirectional RTS transmission by N3 could potentially give rise to collision at N2 during the packet delivery from N1 to N2. This situation could be avoided by restricting the RTS transmission when the channel is idle. In doing so, it would mean that the advantage of parallel communications made possible by the spatial reuse concept could not be achieved as illustrated in Figure 2-8 (b).

To solve this problem, the coordinated directional MAC (CDMAC) protocol [69] proposes the use of a time structure in conjunction with omnidirectional RTS transmission. In the case of CDMAC, the time axis is organised in consecutive frames, each is made up of a contention period followed by a coordination period, as shown in Figure 2-8 (c). Within a contention period, pairs of a sender and its intended receiver would exchange RTS and CTS messages that are being transmitted in all directions. After a successful exchange of the RTS and CTS messages, DATA and ACK can then proceed with directional transmissions within the coordination period. This way of operation is illustrated in a situation as depicted in Figure 2-8 (c) whereby simultaneous data transmissions could be carried out within a coordination period.

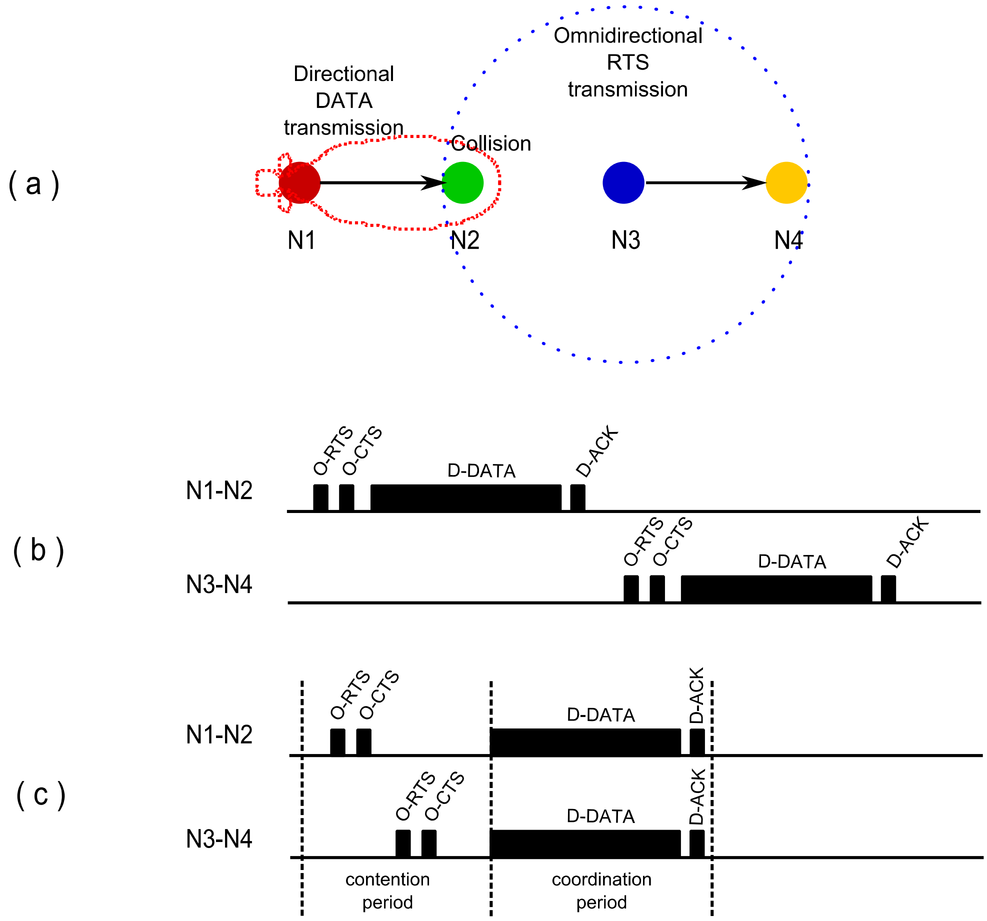

Figure 2-8 Different operating scenarios with CDMAC protocol. (a) possible collision due to omnidirectional RTS transmission, (b) situation that would prevent simultaneous data transmissions by two pairs of nodes, and (c) situation that enables simultaneous data transmissions by two pairs of nodes.

The drawback of protocols that involve the use of directional antennas might be the cost associated with the complex antenna system, particularly for low cost nodes. Therefore, research on directional antennas intended for WSN applications is undertaken in [70-71]. Even though directional antennas developed in [70-71] are low cost, the additional cost may be too significant for a large scale WSN studied in this thesis. Moreover, although the antenna dimension for the operation on frequency of 2.4 GH is relatively small, i.e., 10 cm x 10 cm x 6 cm [70] and 5.6 cm x 5.6 cm x 5.6 cm [71], the dimension will increase significantly for the operation on lower frequencies. For instance, the operation on the frequency of 434 MHz will need an antenna in [70] with a dimension of 50 cm x 50 cm x 30 cm. As a consequence, the antenna construction will be more complex, the production cost will be more expensive, and may cause difficulty and time consuming during node deployment. In addition, deafness problem is still being a drawback of this approach. This problem may be minimized by using omnidirectional antenna at the time RTS being sent [68]. However, it can cause collision and prevent parallel transmission. Meanwhile, utilizing time structure [69] to reduce the effect of deafness problem requires a central control, which is not suitable with distribute control applied in WSN studied in this thesis.

In addition to the approaches described earlier in this section, the effect of hidden node problem could also be overcome or minimized through the use of multiple channels. The aim here is to allow various pairs of sending and receiving nodes to carry out simultaneous transmissions by using one of several available idle channels chosen in a dynamic way. Several of these protocols are reviewed in the following section.

2.5 EXISTING MULTICHANNEL MAC PROTOCOLS FOR ENHANCING MULTIHOP NETWORK PERFORMANCE

Multichannel based MAC protocols have been proposed to overcome hidden node and exposed node problems commonly encountered in a single channel WSN, with the aim to improve the overall throughput of the network. An example of a WSN using multichannel is shown in Figure 2-9 where the distance between two nodes could either be within or outside the transmission range of a given node. In this example, it is assumed that the transmission range of every node is the same. Packet delivery from a source node to a destination node is indicated by an arrow. The channel used by respective pair of nodes is indicated on the arrow.

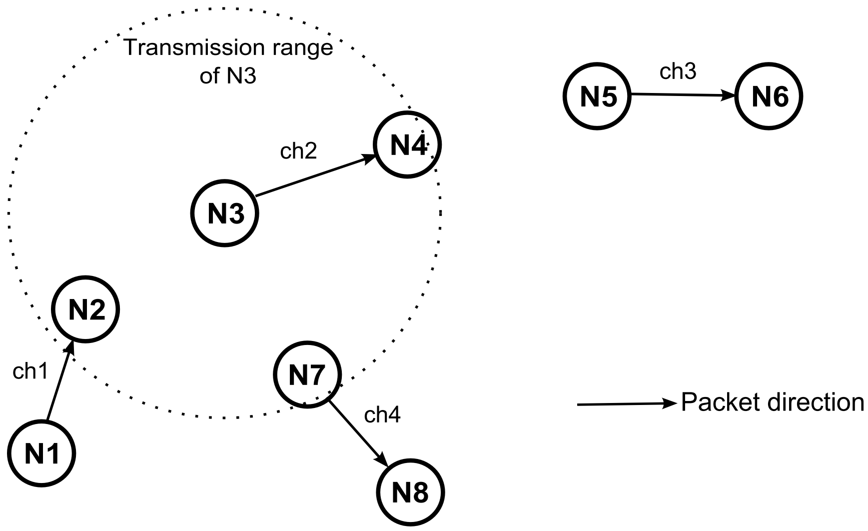

Figure 2-9 An example of a WSN showing inter-node communication links.

Considering that all nodes in Figure 2-9 can use one of available channels, the figure shows current packet deliveries using the chosen channels. With such various channels utilization, collision due to hidden node problem could be prevented. For example, the collision at N2 between N1 and N3 transmissions does not happen as N1 and N3 utilize different channels. Furthermore, simultaneous transmissions could be enabled in the presence of exposed node problem. This is can be seen in N3 and N7 case, where N7 can deliver packet to N8 although it is in the transmission range of N3, that may prevent N7 providing any transmission if the network operates on a single channel. Utilizing multichannel does not always mean that it uses a large number of channels. For efficient bandwidth utilisation, it is common to adopt spatial channel reuse in an attempt to limit the number of channels to be needed by the network.

To enable packet exchange in a chosen channel, multichannel schemes commonly require a sender node and an intended destination node to undertake two stages. In the first stage, such pair of nodes must carry on channel negotiation [27-28], that is also known as rendezvous [27]. To achieve a proper negotiation, the sender and receiver must be in the same channel specified by multichannel schemes. For example, ch0 is used for rendezvous channel of network in Figure 2-9. If a channel has been chosen, both sender and receiver change their transceiver channels to the selected channel and then undertake the second stage, which is a packet exchange. Once the packet exchange has been completed, both sender and destination nodes come back to the rendezvous channel.

Although multichannel schemes could provide beneficial simultaneous transmissions as illustrated in the Figure 2-9, problems accompanied with multichannel, namely deafness and multichannel hidden node, may occur. For instance, a deafness problem could happen at N4 and N5, if it is assumed that N3 is delivering packet to N6 through multihop links N3-N4, N4-N5, and N5-N6. Let the current packet delivery is shown in Figure 2-29. If packet delivery from N3 to N4 has finished, N4 goes to rendezvous channel to prepare packet delivery to N5. Once in the rendezvous channel, N4 sends a request to N5. At this time, N5 probably has just finished its task and has not moved to rendezvous channel. Thus, N5 cannot hear the request from N4. If N4 has sent several requests while N5 has not achieved the rendezvous channel, N4 may drop the request. Apart from this effect of deafness problem, multi request messages transmitted by N4 may increase the rendezvous channel contention, and therefore reduce the possibility of successful simultaneous transmissions.

Meanwhile, multichannel hidden node problem could occur at N2 and N3, if N3 intends to send a packet to N7, after it delivered packet to N4. Let N3 requests channel negotiation to N7 while N1 is still sending packet to N2. N3 and N7 may choose ch1 that is being used by N1 and N2. It is possible if during previous negotiation between N1 and N2, N3 and N7 were not in rendezvous channel. Consequently, once a transmission is started by N3, the collision happens at N2. To prevent deafness and multichannel hidden node problems, or to reduce the effect of these problems, various ways are proposed as addressed in the next subsections.

Furthermore, despite multichannel scheme could alleviate the effect of hidden and exposed node problems, the utilization of this scheme may not be for this purpose. In [28], multichannel scheme is aimed to minimize the effect of interference, and therefore improving the network capacity. Regarding this objective, study in [28] classifies the multichannel protocols into fixed, semi-dynamic, and dynamic channel assignments, depending on the way the channel is assigned to a node. The first type, fixed channel assignment, is aimed to work on a network with high numbers of nodes densely deployed in an area. In this scheme, nodes within a cluster communicate with a fixed channel that is distinguished from the channel used by neighbourhood clusters. This scheme may not be suitable to minimize hidden and exposed node problems as nodes in a cluster use the same channel.

Similar with the fixed channel assignment, each node in semi-dynamic channel assignment has a fixed channel. However, it can change its channel into the neighbour node channel to provide a data exchange. Hence, semi-dynamic channel assignment may be able to reduce the effect of hidden and exposed node problems. On the other hand, each node in dynamic channel assignment can choose any channel dynamically among available channels. Considering that the quality of radio channel in hostile environment of rural area can change dynamically due to the weather, temperature, and humidity, the implementation of dynamic channel assignment may be more appropriate than semi-dynamic channel assignment.

Furthermore, depending on how the channel negotiation process is implemented, protocols employing dynamic channel assignment could be classified into frequency hopping (FH), dedicated control channel (DCC), and split channel (SC) [27-28]. In this thesis, another class namely sensing all (SA), is included as it has different mechanism compared to other three classes. Figure 2-10 shows all categories along with their examples.

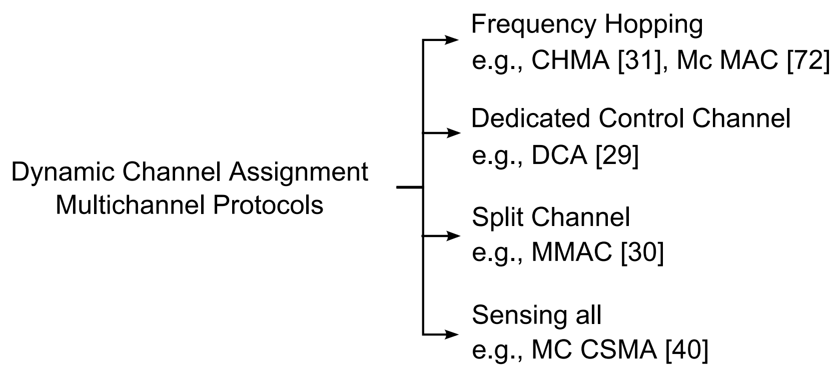

Figure 2-10 Classification of multichannel MAC protocols with dynamic channel assignment

2.5.1 Multichannel MAC Based on Frequency Hopping

In frequency hopping method, each node changes the frequency of its transceiver periodically following the channels sequence predetermined by the protocol. An example of this protocol is Common Hopping Multiple Access (CHMA) [31]. During the operation, all nodes in CHMA are synchronized to change the frequency following the common hopping sequence defined in each node. The length of one hopping period must be long enough to send an RTS packet as shown in Figure 2-11. On the other hand, the data packet can be transmitted within several hopping periods.

<table>
<tr><th>time
freq</th><th>t1</th><th>t2</th><th>t3</th><th>t4</th><th>t5</th><th>t6</th><th>t7</th><th>t8</th><th>t9</th><th>t10</th></tr>
<tr><td>f1</td><td>N1 -> N2
RTS</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>f2</td><td></td><td>N1 <- N2
CTS</td><td colspan="7">N1 -> N2
DATA</td><td></td></tr>
<tr><td>f3</td><td></td><td></td><td>N5 -> N6
RTS</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>f4</td><td></td><td></td><td></td><td>N7<->N8
RTS</td><td>backoff</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>f5</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>f6</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Figure 2-11 Rendezvous and data exchange mechanism in CHMA [34]

In Figure 2-11, nodes referred to network in Figure 2-9, are synchronized to follow a repetitive sequence of six predetermined frequency channels, namely f1, f2, f3, f4, f5, and f6. Each channel lasts for one time slot so this frequency hopping sequence repeats after six time slots. Now, consider that the 3 pairs of nodes: N1-N2, N5-N6, and N7-N8, are ready to exchange data at different hopping time slots. Let assume at time slot t1, N1 wishes to deliver data packet to N2. It first senses whether the predetermined channel, f1, at this particular time slot is idle. If so, it sends an RTS message to N2 via f1. Upon successfully received the RTS, N2 then replies with a CTS to N1 via channel f2 during t2. When this CTS is received, N1 recognizes that N2 is ready to receive the data, and thus it starts to deliver data to N2 using the same channel, i.e., f2, that conveyed the CTS. As shown in Figure 2-11, this delivery of data from N1 to N2 is completed in 7 time slots from t3 to t9. Once the packet transmission is over, both N1 and N2 would return to synchronize themselves to follow the common frequency channel sequence. In this case, the channel f2 is busy at its next common synchronized time slot, t8. As such other nodes will sense that f2 is occupied, and no activity will take place in this channel until the following hopping period, i.e., at time slot t14.

Apart from this successful rendezvous between N1 and N2, the rendezvous for the other two pairs of nodes, N5-N6 and N7-N8, is shown to be unsuccessful. In this example, after N5 sent out a RTS message via f3 at t3, it did not receive the expected CTS message from N6 at f4 during t4. Consequently, N5 would continue to follow the hopping sequence, and could retry the rendezvous in the next hopping period. In the case of the pair of N7-N8, both nodes sent out a RTS message to one another via f4 during t4. This resulted in collision, so both nodes underwent back-off and would repeat the rendezvous process at the next hop. Unsuccessful rendezvous could also happen if N3 sends RTS to N4 at t1. In this case, the collision between RTS packets sent by N3 and N1 happens in N2, causing the failed rendezvous of the pair N3-N4. These three failed attempts in the rendezvous process would lead to longer delay in packet delivery, or even packet drop if the number of retries is exceeded.

Multichannel MAC (Mc MAC) [72] is another type of frequency hopping protocol. Unlike CHMA that all nodes following the common hopping sequence, each node in Mc MAC has its specific hopping sequence, namely home sequence, that is different with the other nodes. The hopping sequence is pseudorandom with the seed is taken from the node MAC address. Through a sharing mechanism, a node in Mc CSMA always sends the information of hopping sequence, the hopping period boundary, and the current hop where the node is setting its transceiver. Therefore, a node in Mc CSMA recognizes all neighbour nodes hopping pattern and period.

By relying on such mechanism, a sender wishing to send packet to a receiver, just needs to switch its transmission channel to the channel of the receiver node, and sends an RTS message. However, before sending the RTS message, the sender senses the receiver channel to ensure that no transmission is in progress. If the channel is idle, the sender runs the random contention window before finally transmits the RTS message. If the channel is currently used, the sender is back to its home sequence.

It can be seen that rendezvous process is performed in receiver node channel. As each node has different hopping sequence, several pairs of sender-receiver can do simultaneous rendezvous that cannot be provided in CHMA. However, a rendezvous collision in Mc MAC may occur if the hopping sequences of the receivers meet at the same channel at the time when the channel negotiations are provided. In this case, the channel rendezvous can be retried at another hopping period.

The discussion on frequency hopping method describes that nodes could not notice activities performed by other pairs when they are exchanging data packet in another frequency. As a consequent, they are vulnerable to deafness and multihop hidden node problems. Moreover, since a channel switching in a transceiver could takes 200 μS [73], a periodic channel switching as in frequency hopping method may reduce the network performance, particularly the network throughput. In addition, as nodes need to have the same hopping period boundaries, a central control is required to broadcast a beacon or synchronization signal. This centralized control may not be suitable for distributed network control studied in this thesis.

2.5.2 Multichannel MAC Based on Dedicated Control Channel

In dedicated control channel (DCC) protocol, each node is equipped with 2 transceivers. A transceiver is used only for exchanging channel negotiation messages in a specified channel. Meanwhile, another transceiver is utilized for data delivery. For this purpose, the transceiver is multichannel and therefore the packet can be delivered via any of the available channels. The advantage of using a dedicated transceiver for control channel is that every node always follows the activities of other nodes while it is in any other channel. Hence, the node knows in which channel the other nodes staying. Consequently, deafness and multichannel hidden node problems could be prevented. An example of DCC is a dynamic channel assignment (DCA) MAC protocol that is described in [29].

With DCA each node maintains a data channel usage list (CUL) and a free channel list (FCL). CUL stores the IDs of neighbouring nodes, the channels being used by neighbouring nodes and their respective time of release after current communications. With the available information on individual neighbouring nodes contained in its CUL, the node then calculates and stores the list of free channels in its FCL. The steps taken to arrive at an agreed channel agreement in DCA is illustrated in Figure 2-12.

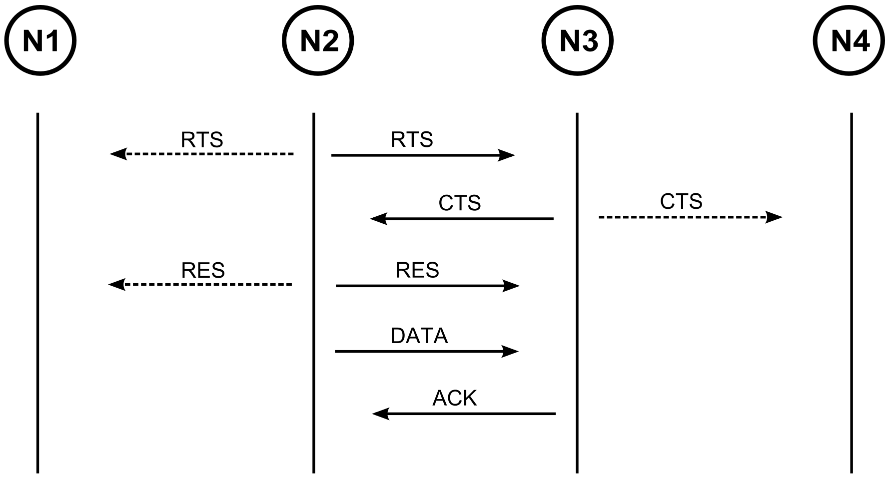

Figure 2-12 Exchanges of control messages to arrive at an agreed channel for data transmission with DCA

Let assume N2 intends to deliver data packet to N3. Node N2 first sends to N3 via the control channel a RTS message containing its FCL and the packet size it intends to send. Upon receiving the RTS, N3 compares the FCL from N2 with its own FCL to find out what are the free channels still available. After a free channel is chosen, N3 replies N2 with a CTS message comprising information of the chosen channel and the network allocation vector (NAV). NAV is typically utilized in 802.11 standard [18] to indicate the length of packet delivery undertaken by a given pair of nodes. Because a CTS message is transmitted by means of broadcast, N4, being an adjacent node of N3, can also receive the CTS message. As a result, N4 withholds its transmission for a CTS NAV period. When N2 receives the CTS from N3, it sends a RES message containing information on the chosen channel as well as NAV. Following this, data will immediately be sent out on the agreed data channel. Being a control message, the RES message broadcast by N2 is able to be heard by its adjacent node N1. Therefore, N1 will withhold its transmission for an NAV period. In this way, data packet could be delivered from N2 to N3 without worry of collision. Furthermore, an acknowledgement packet is still sent by N3 to inform N2 that the packet delivery is received successful.

Although DCC gives an advantage by preventing deafness and multichannel hidden node problems, the use of a separated transceiver for only channel negotiation might be a drawback of this scheme. If the network is not too busy, channel negotiation may rarely occur and hence leads to a low channel utilization. In contrast, during a busy period, channel contention due to high numbers of channel negotiations may cause collisions.

2.5.3 Multichannel MAC Based on Split Channel

For multichannel protocol implementing split channel (SC), a channel is structured into time frames. Each time frame is made up of a control field and a data field. Channel negotiation is taken during a control field. Once a pair of nodes has decided on an agreed data channel, packet delivery will then be carried out in the data field of the agreed channel. Moreover, proper operation would require all individual nodes to be synchronized to the time frames of the channels. One way to achieve such global synchronization, i.e., synchronization for entire network, is to make use of the ad-hoc traffic indication messages (ATIM) timing frame, available in IEEE 802.11 power saving mechanism (PSM) [18].

With IEEE 802.11, all nodes in a network are being synchronized to a periodic beacon transmission from the very first node that forms the network. Each beacon transmission period is separated into ATIM and DATA windows, as shown in Figure 2-13.

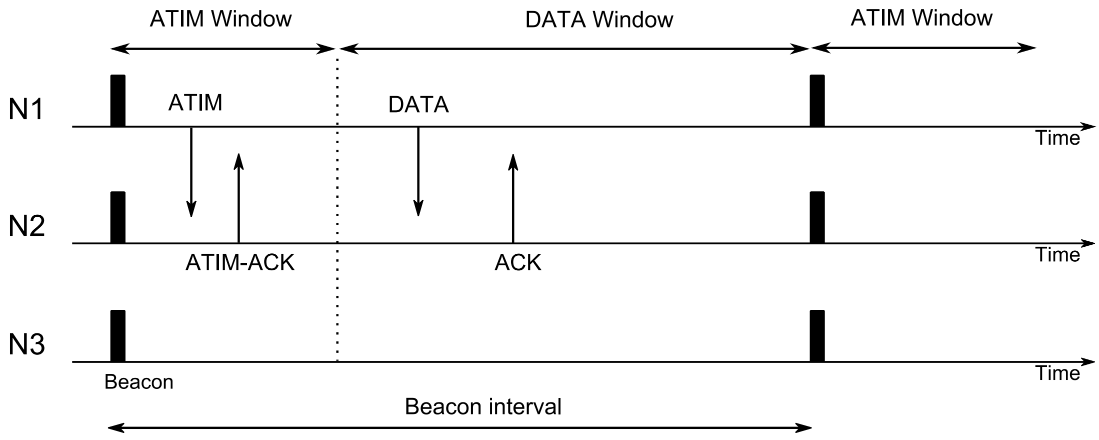

Figure 2-13 ATIM and DATA windows in 802.11 PSM

Now, if N1 wishes to deliver data to N2, it first sends an ATIM message to N2. Upon receiving the ATIM message, N2 replies an ATIM-ACK, in the current ATIM window, to N1. Once the ATIM-ACK is received, N1 can then deliver its data packet to N2 during the DATA window. The data delivery process is complete after an ACK is sent by N2. All these procedures are performed in a single channel communication.

Multi-channel MAC (MMAC) protocol [30] modifies the time frame structure of single channel 802.11 PSM into one that could support multichannel transmissions, as shown in Figure 2-14. In this case, during the ATIM windows, all nodes are tuned to the pre-specified control channel. A beacon and ATIM messages are exchanged within this ATIM window. ATIM messages are made up of modified ATIM and ATIM-ACK packets, and an additional ATIM reservation (ATIM-RES) packet. Meanwhile, RTS/CTS messages are included in data delivery process performed within a DATA window. After a successful rendezvous within an ATIM window, the packet delivery can then take place in any conformed channel including the control channel, which is not used for rendezvous within its DATA window.

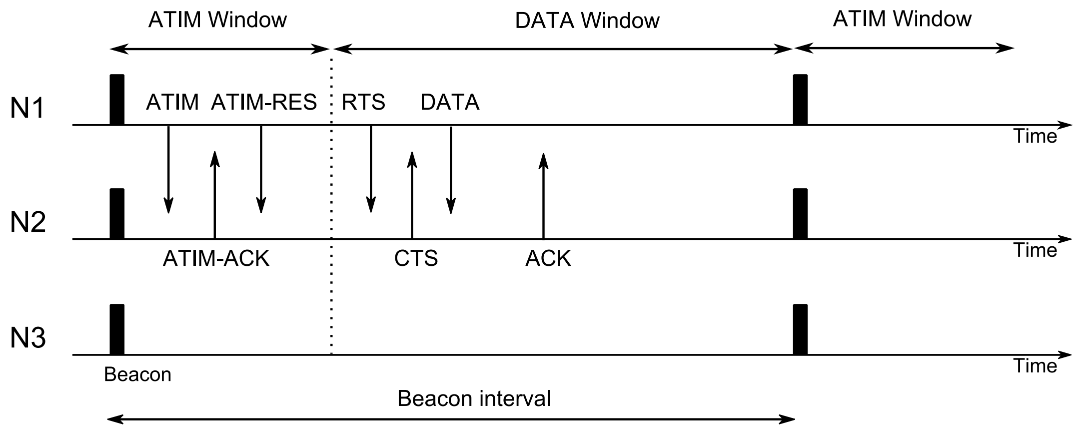

Figure 2-14 Control and data exchange mechanism in MMAC

With reference to Figure 2-14, if node N1 intends to deliver data to destination N2, an ATIM message consisting of its preferred channel list (PCL) is first sent by N1 to N2. Upon receiving this control message, N2 compares the offered PCL with its own PCL. Once a data channel has been decided, N2 returns to N1 an ATM-ACK message consisting the information of the chosen channel. If N1 agrees to use this chosen channel, it sends an ATIM-RES packet to N2. Afterwards a series of RTS-CTS-DATA-ACK exchanges between N1 and N2 take place within the DATA window of the chosen channel. In the event that N1 does not agree with the channel chosen by N2, it would provide another channel offer in the next ATIM window. In addition, if the size of a data packet is too large to be sent within a single DATA window, it would be broken up into several shorter packets to be delivered using the next few consecutive data windows.

Furthermore, NAV is included in all the control messages, such as ATIM, ATIM-ACK, RTS, and CTS, to provide information on the data transmission period between a pair of nodes, so that hidden nodes would be able to decide on how long they should hold back from transmitting. However, since the rendezvous process takes place only in a single channel, transmissions of control messages within an ATIM window from different pairs of nodes may collide with one another. One way to improve the channel negotiation reliability is for a sending node to perform a random back off before resending an ATIM message. Nevertheless, the use of a single channel for rendezvous would produce too many contentions between various pairs of nodes. This is a disadvantage of MMAC. Another disadvantage is that data channels are not used during ATIM window. This leads to the waste of channel resources.

To improve the performance of SC based MAC, several protocols have been proposed to overcome drawbacks of MMAC. One of them is Hybrid MMAC (H-MMAC) [74] as described as follows. Based on the concept of SC, H-MMAC also makes use of idle ATIM windows for data transmission. This is achieved by maintaining two tables, Neighbour Information List (NIL) and Preferable Channel List (PCL) in every node. NIL contains the neighbour's ID, state, type, and transmit (Tx) Mode, which is specified as either normal transmission (N-Tx) or extra transmission (E-Tx) depending on the size of the packet to be transmitted. For example, N-Tx is specified if the data packet can be sent out within a single DATA window. Otherwise, E-Tx is specified for longer data packets. This information together with that for the chosen channel are included in the ATIM-RES message exchange for the transmission of a large data packet between a pair of nodes. Consequently, neighbouring nodes would withhold transmitting during the DATA windows on the respective channel. Simulation results carried out in [74], based on a network of 36 nodes and 8 channels, show an 18 % increase in throughput obtained by H-MMAC compared with MMAC.

Channel Traffic Balance MAC (CTB-MAC) [75] has been proposed not only to make use of any idle ATIM window for data transmission, as in H-MMAC, it also attempts to reduce the likelihood of collisions in control message exchanges during the ATIM window. As for MMAC and H-MMAC, a beacon period in CTB-MAC is also divided into ATIM window and DATA window. However, the DATA window in CTB-MAC is divided into several timeslots, each has the same interval as an ATIM window. This applies to all channels rather than just to is a specific channel as in MMAC and H-MMAC. Figure 2-15 shows the arrangements of ATIM and DATA windows within a beacon period for CTB-MAC.

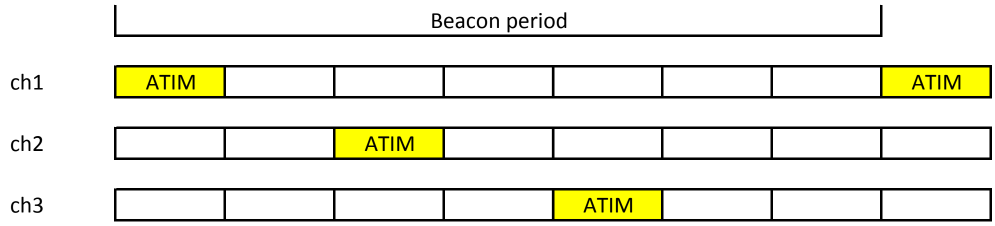

Figure 2-15 ATIM and DATA windows in CTB-MAC

Unlike MMAC and H-MMAC, each node in CTB-MAC stays at a particular channel, also referred to as the home channel, for the entire duration of its operation during the operation. A node will only leave its home channel if the destination node is located in another channel. A number of nodes may share a home channel. However, nodes are distributed such that each home channel is shared by more or less the same number of nodes. This is done to try to balance the traffic loads evenly among the available channels.

To start a data delivery process, the sending node will move to the home channel of the destination node to exchange the ATIM messages during the ATIM window. Note that the same ATIM messages are used in MMAC and H-MMAC. If the pair agrees to perform data delivery, then an ATIM-RES is broadcast to other nodes sharing the same home channel, informing them that the number of time slots have been reserved for a specified period. Following this successful handshake, data delivery can then be carried out within the DATA windows. It is shown in [75] that CTB-MAC is able to achieve an 128 % increase in throughput, and 67 % higher in channel utilization when compared with MMAC.

The use of ATIM window only for channel negotiation could eliminate deafness and multichannel hidden node problems as all nodes are in the same channel. However, it might be inefficient in term of channel utilization. On the other hand, enabling data transmission during ATIM window could improve the channel utilization. Nevertheless, it may cause deafness and multichannel hidden problems, as nodes exchanging data are not in the rendezvous channel. As such, a treatment is required to obtain an optimum performance. Furthermore, it is described that SC based protocol relies on beacon. If the beacon is generated by a central station, it is not suitable with the network studied in this thesis as the network uses distributed control. The beacon may be generated by a distributed control as in independent basic service set (IBSS) network in 802.11 standard [18]. However, it may become another communication overhead along with the channel negotiation itself.

2.5.4 Multichannel MAC Based on Sensing All Mechanism

Finally, multichannel MAC protocols incorporating “sensing all” are considered here. With this type of protocols, there is no channel negotiation as is required by previous three protocols. Instead, every node of the network is equipped with multiple receivers so that it could listen to all the available channels simultaneously. Multichannel carrier sense multiple access (MC CSMA) [40] is one of such protocols.

With MC CSMA, each node has to maintain a free channel list and a last-channel list. The former contains a list of idle channels, and these are channels with values of received signal strength falling below a given sensing threshold. Meanwhile, the last-channel list is made up of those channels that have successfully delivered their last data packets.

When a node is preparing to send a data packet, it first looks for any idle channel in its free-channel list. If one or several idle channels are available in the list, then a check is carried out to see whether any of these channels is the same as the one currently stored in the last-channel list. If it is, then data delivery will be carried out on this channel. Otherwise, an idle channel in the free-channel list will be chosen on a random basis. On the other hand, if the free-channel list is empty, the node will wait until the first channel becomes idle within a long inter frame space (Long IFS) period.

The channel that is used for successful packet delivery is then stored in the last-channel list of the sending node. If the packet transmission can be undertaken and successful, the channel is stored by the sender into the last_channel. This channel will also form the reserved channel for the next packet transmission. However, if the packet delivery is unsuccessful, then the concerned node will undergo a random back off before retrying to send the data again.

In [40], a simulation is arranged to derive the performance of MC CSMA scheme in comparison with a single channel scheme. Result shows that the throughput of the network using MC CSMA can achieve more than 2 times the throughput of network using a single channel, for number of channel more than ten. This result may be reasonable, as this protocol is applied for a network that consists of n^2 nodes deployed in n x n square grid, where most of nodes can reach other nodes in a single hop transmission. Thus, it is difficult to reduce the number of channel by, for instance, spatial reuse. However, if MC CSMA is evaluated in long chain multihop networks as in Tier 2 and Tier 3 of the WSN architecture studied in this thesis, the number of channel, i.e., receiver, could be reduced as spatial reuse can be applied in conjunction with MC CSMA.

Despite the use of multi receiver that may be costly, particularly for a large scale network, sensing all schemes have some advantages. First, it does not need rendezvous, and therefore could reduce communication overhead. As a result, the throughput could be increased. Second, the utilization of multiple receiver can eliminate the requirement of synchronization mechanism as needed by FH and SC protocols. Thirdly, a simultaneous channels sensing or receiving undertaken by multiple receiver may alleviate the possibility of deafness and multichannel hidden node problems. With such advantages, this sense all method may be suitable to be implemented in networks in Tier 2 and Tier3.

Furthermore, it can be seen that each node in MC CSMA chooses its channel only based on the channel used by neighbouring nodes. It does not consider the channel used by nodes 2 hop away. Hence, the effects of hidden and exposed node problems may still occur. Therefore, a new sense all protocol is proposed in Chapter 3. This protocol is able to set up transmission channel used by nodes 2 hops away to reduce the effect of hidden and exposed node problems. With this ability, the new protocol is expected can have a better performance compared to MC CSMA.

2.6 ESTIMATING THE CAPACITY OF WIRELESS ADHOC NETWORKS AND WIRELESS SENSOR NETWORKS

Network capacity is an important parameter to measure the capability of a network in delivering information. An actual capacity of a network is derived through a measurement. However, the capacity of the network could be estimated using mathematical models. In these models, various factors such as network topology, protocol, interference, and transmission power, are investigated to look at their effects on the network capacity. Other parameters such as weather and type of environment, e.g., city, urban, forest, may be included to study network capacity in a specific environment.

For three-tier network studied in this thesis, it is important to estimate the capacity of networks, particularly those in Tier 2 and Tier 3 of network architecture shown in Figure 1-1 of Chapter 1. This is because networks in these tiers must be able to deliver packet from SNs to CS in any situation including in an emergency situation, where the data rate generated by SNs is significantly high. For this purpose, an accuracy of the capacity prediction is important. Inaccurate estimation may cause, for instance, an underestimated maximum capacity. Consequently, when the network is implemented, an overwhelmed data rate during emergency situation may cause traffic congestion that significantly reduces network reliability.

Nowadays, such mathematical models could be solved using computer simulation. Based on computer simulation, various prediction methods have been proposed such as in [33 - 35]. These methods are adopted by other researchers, and probably could be used to estimate the capacity of networks in Tier 2 and Tier 3, if they are able to predict the capacity of irregular networks available in those tiers. As described in Chapter 1.1 of Section 1, most networks in Tier 2 and Tier 3 will be on irregular tree topologies consisting long chain multihop networks. In irregular tree topologies, the location and number of branches will be asymmetrical. Hence, it may require a mathematical model that is more complex than the mathematical model of regular topology such as symmetrical tree [36], grid and ring [37], and two dimensions square network with infrastructure [38] that have a regular shape. Furthermore, it is also desired a simple method that is able to provide a fast estimation result. It will be useful if during network deployment in the field, the topology often changes due to unexpected environment situation. This possibly happen in a hostile environment such as in the jungle in Kalimantan Island, where the environmental WSN will be deployed. Moreover, as location of SNs cluster could prone to different disaster, the traffic data rate generated by SNs cluster may different to each other. Therefore, the estimation method should be able to predict a network throughput under various data rate.

A method that is referenced by several studies is proposed by Gupta and Kumar [33]. They define the capacity of a network as a number of possible parallel transmissions provided by *n* nodes in a specified area. This method can derive the maximum and minimum capacity bounds of a network. Furthermore, a network in this method can be configured based on two scenarios so called arbitrary and random networks. In arbitrary network scenario, nodes are arbitrarily deployed in a disk of unit area. Each node chooses an arbitrary destination to perform a source-destination pair. Arbitrary power level is chosen for each transmission. On the other hand, in random network scenario, nodes are randomly allocated. Unlike the arbitrary network, each node has the same power transmission and choose its destination randomly. Moreover, to determine a successful transmission, Gupta and Kumar utilize two different wireless channel models that are called protocol and physical models. In a protocol model, packet delivery from a sender to a destination is successful if distance between them is shorter than the distance between the destination and another transmitting node. If this condition is satisfied, transmission from another node will not interfere the packet transmission from sender to the destination. In physical model, packet delivery from a sender to a destination is successful if SINR at the destination node is higher than the SINR threshold.

According the description above, the method introduced by Gupta and Kumar consider only a grid or mesh topology, where the nodes are distributed within an area. The method also considers only a symmetrical traffic pattern where the traffic is distributed uniformly among the node. The topology and traffic pattern are different with those used in this thesis. In Tier 2 and Tier 3, the network performs irregular tree topology comprising long chain multihop network. Meanwhile, the traffic flows from twigs to the trunk, causing more possibility of collision at a node joining two traffics. As a result, the capacity of this network is lower than the capacity of network assumed by Gupta and Kumar. This has been proven by Haddad and Riedi [36]. In their study, Haddad and Riedi find that Gupta and Kumar method can overestimate the achievable throughput when it is implemented in several topologies and traffic patterns. This is because the topology and traffic pattern assumed by Gupta and Kumar are often diverged from those in a real network.

Nonetheless, Haddad and Riedi [36] consider that Gupta and Kumar method could be enhanced by taking the topology into an account. However, Haddad and Riedi discover that graph-based approach used by Gupta and Kumar tends to derive a very complex formulation if the topology is incorporated. This is because the approach attempts to configure all possible connections between sender and destination nodes by considering a minimum distance between senders that avoids interference. Therefore, Haddad and Riedi introduce a different approach that can untangle mutual interferences among simultaneous transmissions, which is called space-based approach.

A space-based approach basically divides the entire network area into several sub areas that are called transmission arena. Reference point of a transmission arena is determined by an arbitrary point X. The area of the arena is bounded by a radius r, that is longer than transmission radius of anode. Then, it is assumed the senders are located on r, and all senders have the same transmission radius. As such, a maximum number of simultaneous transmissions could be derived by calculating number of senders that their transmission coverage does not disjoint to each other. Then, the capacity bound of an arena could be derived by multiplying number of simultaneous transmission with the data rate of each node. Therefore, it can be seen that the capacity bound of an arena is based on the radius of the arena and the transmission radius of the node, e further developed to obtain a topology sensitive capacity bound. This approach could be further developed to calculate the capacity of network with a specific topology by utilizing Euclidian Minimum Spanning Tree (EMST), rather than the curve connecting all senders as described above. To examine this approach, Haddad and Riedi apply it on clustered topology network. The result shows that their estimation result is tighter than the result derived by Gupta and Kumar.

Nevertheless, an improvement proposed by Haddad and Riedi is used to estimate a regular topology. It is possibly due to uniform shape of the regular topology that can be represented by a simpler mathematical model compared to the mathematical model of irregular topology. Moreover, Haddad and Riedi still assume that nodes generate the same data rate as in Gupta and Kumar method. Therefore, the methods proposed by both pairs are still not able to predict the capacity of network with irregular tree topology, and the network with heterogeneous data rate.

Meanwhile, an estimation method proposed by Kleinrock and Silvester [34] studies a correlation between network capacity and transmission radius on a packet radio network. In this method, a network is configured by a number of randomly deployed nodes with uniform distribution in a specified area. Every node has the same transmission radius and traffic load. Each node randomly chooses a destination to form a source-destination pair. Once the destination has been chosen, a packet transmission is undertaken within a time slot that is set up by slotted ALOHA protocol. Every sender has the same probability to access each time slot available in slotted ALOHA. A successful transmission is achieved by a pair if there is no interference affecting their transmission. The network throughput then is determined by accumulating number of successful transmissions over the entire network at each ALOHA slot for a given time. For multihop transmission that takes more than one ALOHA slot, the throughput is determined by dividing accumulated throughput by number of repeated transmission. The study derives that the throughput decreases when transmission radius increases. This is because a longer transmission radius may cover more nodes that intend to do simultaneous transmission. Consequently, such nodes cannot undertake transmission as they sense that the channel is busy. If the transmission radius is reduced, the throughput may increase. However, more reduction on transmission radius may cause more number of hops between source and destination nodes. As a result, internal traffics increases and may decline the network capacity due to more collision. Moreover, a smaller radius may disconnect some links, as the distance between a source and a destination is more than the transmission radius, while there is no intermediate node between them. To obtain a maximum throughput, it is required to set an optimum transmission radius. In this study, the optimum radius is determined by number of neighbouring nodes covered by transmission radius. The authors find that six neighbour nodes within a transmission radius can give a maximum throughput.

With the description addressed above, it can be seen that the topology assumed by Kleinrock and Silvester is similar with the topology used in Gupta and Kumar study. With such an assumption, this method may derive an over estimate result as has been studied by Haddad and Riedi [36]. Hence, a modification is required to include a mathematical model of the topology into the calculation. However, for irregular tree topology used in Tier 2 and Tier 3, the representing mathematical model might be too complicated. Hence, it will be worthwhile to provide an estimation method that able to estimate the throughput of irregular tree topology in a simpler way. Moreover, as like in Gupta and Kumar method, Kleinrock and Silvester also assume that all nodes generate a uniform data rate. Again, this assumption is not suitable with the requirement of this thesis. As such, this estimation method needs another modification to include calculation for heterogeneous data rate.

Another different approach on network capacity estimation is proposed by Toumpis and Goldsmith [35]. Rather than relying on nodes allocation in an area as proposed by previous methods, their method calculates network capacity based on the network communication scheme. A communication scheme is a collection of rules that establishes data exchange between nodes. In this method, every rule is represented by a rate matrix that defines a relation between sender and destination nodes. The dimension of a rate matrix is n x n if the network consists of n nodes. In rate matrix, each node has two identities. Those are A_i and A_j that determine the node's role as a sender and a receiver respectively. The element of rate matrix is either r, $-r$, or 0. Element r describes that destination A_j receives information from an original sender A_i with the data rate of r. Meanwhile, $-r$ determines that A_j

transmits information with the data rate of *r* that is originally sent by A_i. On the other hand, 0 determines no relation between two identities.

Furthermore, number of matrices in a rule collection indicates the level of protocol restriction. Hence, a flexible, i.e., less restrictive protocol will have a large number of matrices in its collection. As the information net flow can be calculated from weighted sums of basic rates matrices, the network capacity can be derived from the convex hull of a set of basic matrices. However, a rate matrix that has a negative off-diagonal element will not be included in the calculation. Such a matrix is commonly a result of an unstable communication and may be caused by indirectly routing.

In their study, Toumpis and Goldsmith investigate the capacity of a network with a communication scheme consisting rules of variable-rate transmission, power control, successive interference cancellation, single and multihop routing, and spatial reuse. Energy constraint network, network mobility, and time-varying flat fading channels are other rules addressed in this study. For further investigation, Toumpis and Goldsmith incorporate network topology into their scheme. Topologies such as uniformly distributed random topology, line topology, and ring topology are used as the examples in this study.

Considering the ability of the method in incorporating various communication schemes, it can potentially estimate the throughput of network studied in this thesis. For example, this method is able to estimate the throughput of a network with heterogeneous data rate. Also, this method has been evaluated to predict the throughput of network with various topologies. However, all topologies evaluated in this method are regular, and thus can be represented by a few number of matrices. On the other hand, the irregular shape of topologies studied in this thesis may need more matrices. Also, a large scale network utilized in this thesis could derive a large matrix dimension. As a result, the matrices might be too complicated.

The observation of several estimation methods above shows that most of methods assume a mesh topology with its traffic flows in arbitrary direction. This assumption is not suitable with the topology and traffic flow studied in this thesis.

Consequently, the estimation result could be under or overestimate. Other methods proposed in [35, 36] take topology into an account. However, they tend to use regular topologies to reduce the complexity of the mathematical operation. Thus, for such methods, the estimation of irregular topologies may lead to a complicated calculation. Furthermore, undertaking a complicated calculation may take a time and therefore may not be able to derive a fast result, if an estimation is required in the field.

To provide a fast estimation result for irregular topologies in Tier 2 and Tier 3, an estimation method is proposed in Chapter 4. This method uses a simple mathematic operation. Therefore, it is able to derive a fast estimation result. Moreover, as this simple method is purposed to work on multihop network with any branch location, it is suitable to estimate irregular tree topologies in Tier 2 and Tier 3. In addition, this simple estimation method is also able to estimate the throughput of network with heterogeneous data rate. The detail of the method is discussed in Section 4.2 of Chapter 4. Meanwhile, the accuracy of this method is evaluated in Section 4.3, 4.4, and 4.5 of Chapter 4.

2.7 BIDIRECTIONAL PACKET TRANSMISSION IN WIRELESS SENSOR NETWORK AND PRIORITY SUPPORT

In WSNs, packet transmission generally flows only from SNs to CS, which is in this thesis referred as forward traffic. However, packet transmission flowing from CS to SNs, namely reverse traffic, is often required in some applications. For instance, in precision agriculture [79], smart grid [80], and industrial [81] applications, reverse traffic carries command packets to control actuators. The reverse traffic may be still necessary although a WSN is not equipped with actuators. In environmental WSN studied in this thesis, reverse traffic is required to carry command packets to provide remote network supervisory and management. By using this application, CS could send command messages to nodes in network in order to provide tasks such as query driven data report [82], network topology reconfiguration, or routes change. With this capability, the need of in-site attendance could be reduced significantly, and therefore can decrease the maintenance cost.

For environmental WSN studied in this thesis, appearance of reverse traffic is less than the appearance of forward traffic. Forward traffic still occurs more frequent as it sends data report periodically or by request. Therefore, instead of creating an additional channel [83] for the reverse traffic, the existing channel utilized by the forward traffic can be shared for both traffics. Nevertheless, in the presence of both traffics in the channel, reverse traffic is desired to have a better packet delivery than forward traffic. This is because reverse traffic carries command packets that have an important role in a successful network management. Hence, a higher priority is required to give to reverse traffic when both traffics is contending the channel. Next paragraphs address several scenarios describing the importance of high priority assignment for the reverse traffic.

Consider a chain network with n hops. Node N0 is located at the beginning of the chain while node Nn is located at the end of the chain. N0 is the source of forward traffic packet, as well as the destination of the reverse traffic packet. Similarly, Nn is the source of reverse traffic packet, as well as the destination of the forward traffic packet. With two traffic sources, various data rates generated by such two sources could affect the effectiveness of reverse traffic in reaching N0.

If two packet sources in the chain network generate the same low data rate, both traffics could achieve a high packet delivery as the total traffic may be below the maximum network capacity. If the data rate increases, packet delivery of both traffics may reduce as the channel capacity is limited. The packet delivery of both traffics then may stay at the lowest as the throughput of both traffics is saturated at the maximum network capacity. As both reverse and forward traffics generate the same data rate, their packet delivery might be similar for all situation described above. Hence, as it is desired that packet delivery of reverse traffic must be higher than the packet delivery of forward traffic, a higher priority to access the channel is required to give to reverse traffic.

A different situation may occur if data rate of reverse traffic is lower than the data rate of forward traffic. As the data rate of forward traffic is significantly high, this traffic may dominate the channel occupation and leaves a short time idle channel that can be used by reverse traffic. If reverse traffic could deliver most of its packets within such short period, its packet delivery may be high. However, if reverse traffic cannot deliver most packets within such period, its packet delivery may reduce, and below the packet delivery of forward traffic. Thus, a priority support scheme is even more important to apply in this particular case. A method to give the reverse traffic a higher priority is discussed in the next paragraphs.

Prioritizing certain traffic to access common medium under contention based protocol is known as service differentiation [84]. This method consists of two stages which are priority assignment and differentiation. The assignment stage may determine the packet priority based on traffic class, source type, or data delivery model, which refers to static assignment. The packet priority could also depend on packet's remaining hop count, traversed hop count, packet deadline, remaining energy, or traffic load. This refers to dynamic assignment. Both static and dynamic assignments might be combined to perform a hybrid assignment. For example, packet from a certain source with shorter deadline time is given a high priority to ensure this packet can reach its destination before it is dropped.

Once the priority has been determined, the differentiation stage performs a service that distinguishes the chance of each type of packet in accessing the channel. It might be carried on by giving different inter frame space (IFS) and contention window (CW) size as applied in 802.11e standard [39]. This standard is proposed to perform quality of service (QoS) based data delivery that is not available in previous 802.11 standard. To achieve such an objective, arbitrary IFS (AIFS) is introduced to complement the existing short IFS (SIFS), distributed coordination function IFS (DIFS), and point coordination function IFS (PIFS). Time frame comparison of all IFSs is shown in Figure 2-16.

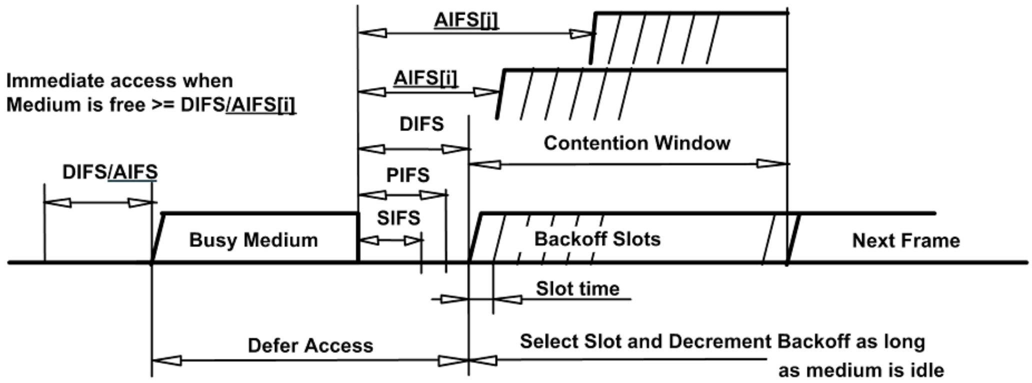

Figure 2-16 Time frame comparison of all IFSs [41]

The size of AIFS and respected CW is defined depending on the packet access category (AC) that is tabulated in Table 2-1. Regarding the table, voice packet has the highest priority followed by video, best effort and background packets. With AIFS number (AIFSN) is 2, the AIFS size of the voice packet is SIFS + 2 * slot time. If the network employs 802.11b protocol with a slot time of 20 micro seconds, the AIFS of a voice packet is 50 micro seconds. Similarly, the AIFS size of the background packet is 150 micro seconds. Furthermore, since the size of allocated CW minimum (CWmin) of 802.11b protocol is 31, the size of CWmin for the voice packet is 7. It means that after waiting for 50 micro seconds AIFS period, a voice packet might be transmitted between 0 to 140 micro seconds. On the other hand, a background packet might be transmitted between 0 to 620 microseconds after waiting for 150 microseconds AIFS period. Such a shorter waiting time could allow the voice packet occupying the channel faster than the background packet. As a result, the throughput a voice packet could be higher than the throughput of background packet. This approach can be applied to bidirectional traffic studied in this thesis.

Table 2-1 The allocations of AIFSN for each of the four traffic categories in 802.11e standard

Packet type	**AC**	**AIFSN**	**CWmin**	**CWmax**
Voice	AC_VO	2	(aCWmin+1)/4 - 1	(acWmin+1)/2 - 1
Video	AC_VI	2	(aCWmin+1)/2 - 1	aCWmin
Best Effort	AC_BE	3	aCWmin	aCWmax
Background	AC_BK	7	aCWmin	aCWmax

There are several studies observing the effectiveness 802.11e in performing priority under distributed coordinated (i.e. adhoc) multihop network. Studies in [85-87], for instance, investigate the fairness derived by chain network in delivering packet types specified in Table 2-1. The result shows that under un-saturated traffic the throughput of various packet type is similar. However, when the traffic is saturated, the higher priority packet obtains the higher throughput. Nevertheless, the studies above do not address service differentiation for reverse and forward traffics as investigated in this thesis, particularly if the data rate of reverse traffic is much lower than the data rate of forward traffic.

To investigate the effectiveness of the AIFS and CW differentiation for two different traffic directions, a simulation using NS3 is carried out in Section 5.3 of Chapter 5. The simulation observes packet delivery rate of both forward and reverse traffics for a 7 hops chain network. Under 802.11b protocol, the assignment of AC type is specified in Enhanced Distributed Channel Access (EDCA) protocol operation available in wifi module. In the simulation, AIFS and CW of voice packet are assigned to reverse traffic, while AIFS and CW of background packet are assigned to forward traffic.

For symmetric situation where both traffics have the same data rate, packet delivery of reverse traffic slightly increases, while packet delivery of forward traffic slightly decreases. On the other hand, for asymmetric situation where the data rate of reverse traffic is much lower compared to the data rate of forward traffic, such a small improvement cannot elevate the packet delivery of reverse traffic above the packet delivery of forward traffic. Hence, it is required another priority support that can provide reverse traffic packet delivery higher than forward traffic packet delivery.

The utilization of 802.11e protocol in the second scenario might be less effective as the data rate of forward traffic is too high. Therefore, even though reverse traffic has a shorter AIFS and CW than forward traffic, it may still hardly contend with a flooding forward traffic to access the shared channel. By considering this possible situation, reverse traffic may have more opportunity to occupy the shared medium if the forward traffic is suppressed. This can be derived by exploiting RTS/CTS protocol [18] as addressed in Section 5.4 of Chapter 5. This section, addressed how RTS/CTS protocol is used to support a priority scheme.

2.8 SUMMARY

This section discusses various factors challenging the deployment of WSN in rural area, where groups of SNs and associated sinks are spread in such an isolated area, whereas the CS is located in the city separated hundreds of kilometres away from the group of SNs. Due to the absence of public telecommunication services, a multitier WSN architecture with multihop communication links can be employed to establish the communication between various locations as described in Section 2.2. However, it has been reported that multihop network suffers throughput degradation due to hidden and exposed node problem as addressed in Section 2.3. Therefore, it is important to enhance the performance of multihop network.

Various methods to improve the performance of multihop network by minimizing the effects of hidden and exposed node problem are discussed in Section 2.4. Those methods are implemented in MAC layer, as this layer has an important role in packet delivery. Among them, multichannel based protocol addressed in Section 2.5 has attracted many attentions as this method can provide simultaneous transmissions through given difference channels. This ability can reduce the effect of the hidden and exposed node problem.

Furthermore, computer simulation is commonly used to investigate the performance of wireless network including WSN. Regarding this, various network capacity estimations have been published. Several are addressed in Section 2.6 to look at their possibility in estimating the capacity of irregular networks in Tier 2 and Tier 3 of WSN architecture studied in this thesis. As those methods are not purposed to predict the capacity of irregular topology such that studied in this thesis, a modification must be provided to the methods. Nevertheless, the modification needs more complicated calculations that may not be able to provide a fast prediction result. Therefore, a simple estimation method that can deliver a fast result is proposed in Chapter 4.

Finally, the WSN studied in this thesis incorporates an additional traffic so called reverse traffic that has an opposite direction of the existing traffic so called forward traffic. As reverse traffic has an important role in providing a successful network supervisory and management, its packet delivery must be higher than the packet delivery of forward traffic. Section 2.7 addressed several techniques that may be suitable for situations in this studied WSN.

CHAPTER 3

2-HOP CHANNEL RESERVATION MAC FOR IMPROVING MULTIHOP NETWORK

3.1 INTRODUCTION

As addressed in Section 1.1 of Chapter 1, an environmental WSN proposed in this thesis comprises of multihop networks. Most network configuration might be dominated by long chain topology due to long distance between source and final destination nodes in the respective tier. For example, the distance between furthest BN and CS in tier 3 could reach over 900 kilometres, which requires more than 15 BNs to connect them. Meanwhile, the topology in tier 2 might be more complex, as high number of SNs cluster locations could combine many long chains into a tree topology. Due to various cluster locations, it could be derived many asymmetrical tree topology configurations in the network. Regardless these various configurations, the use of multihop network in establishing a communication link within hostile forest environment fulfilled with rough elevation and dense vegetation can give flexibility and ease deployment.

Nevertheless, multihop networks suffer from hidden and exposed node problems that could decline the network throughput, as addressed in Section 2.3 of Chapter 2. To minimize the effect of hidden and exposed node problems, various methods are proposed as discussed in Section 2.4 of Chapter 3. Among them, multichannel schemes are often used as they can perform simultaneous transmissions within a local area that can significantly enhance the network performance. This chapter discusses a proposed multichannel scheme that can be classified into sensing all technique. It is developed to improve the throughput of multihop network by minimizing the effect of hidden and exposed node problem. In this thesis, the proposed multichannel MAC employs only two channels to alleviate the effect of hidden and exposed node problems occurring in chain and tree topologies as described in Section 3.2. The algorithm of MAC is described in Section 3.3. In order to examine the performance of the proposed MAC, computer simulation is arranged with the simulation setup addressed in Section 3.4. The simulation result then is discussed in Section 3.5.

3.2 TWO CHANNEL SCHEMES FOR ENHANCING MULTIHOP NETWORK PERFORMANCE

The network architecture proposed in Section 1.1 of Chapter 1 comprises of long chain multihop networks. Several branches on the chain topology may perform tree topology. As it has been known that multihop networks suffer from throughput degradation due to hidden and exposed node problems as described in Section 2.3, this section discusses how a utilization of two channels can solve the effect of such problems, and therefore can improve the throughput of multihop networks. Figure 3-1 (a) illustrates a collision at N2 as N3 transmission to deliver packet to N4 collides with N1 transmission that delivers packet to N2. If a different channel, i.e., ch2, is used by N3 to send packet to N4, the collision due to hidden node problem can be avoided, as shown in Figure 3-1 (b).

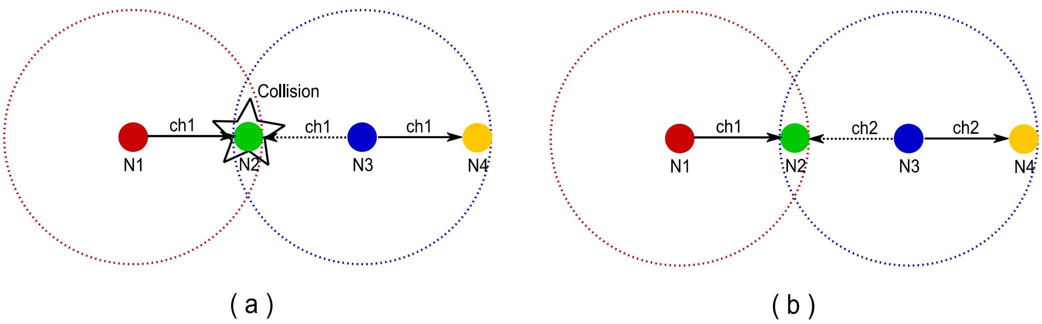

Figure 3-1 A two channels approach to prevent collision by hidden node problem

Furthermore, the 2 channels utilization can also solve the exposed node problem as denoted in Figure 3-2 (a). If the network employs only a single channel (i.e., ch1), N3 cannot send packet to N4 during data transmission from N2 to N1 as N3 senses that the channel is busy. However, if N3 utilizes another channel, i.e., ch2, the data packet can be transmitted to N4 without disturbing the packet delivery from N2 to N1. Thus, the simultaneous transmissions can be established, and consequently, the network throughput can rise.

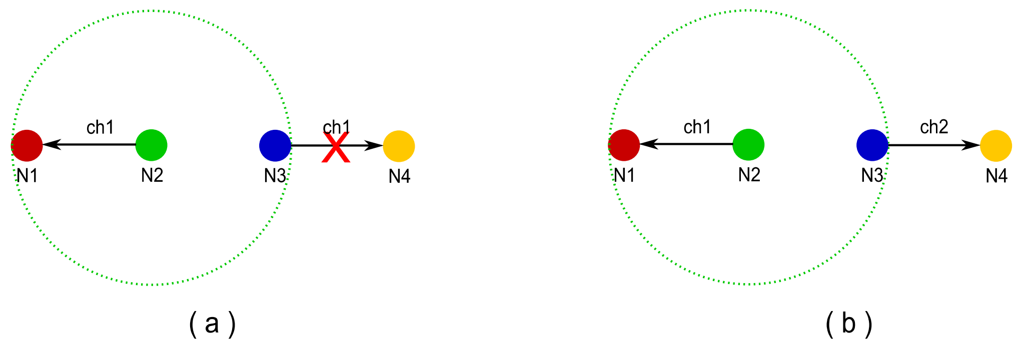

Figure 3-2 A two channels approach to allow exposed node transmitting packet

For a long chain topology, channel selection of every node can be configured as shown in Figure 3-3. Firstly, N1 is the source of the packet and therefore can choose any of 2 available frequencies to transmit its packet. If N1 chooses ch1, N2 can still utilize ch1 as it will not transmit at the time when N1 is transmitting. However, N3 which is 2 hops away from N1, must transmit through ch2 to avoid collision, if N1 is transmitting at the same time. Furthermore, N4 can also use ch2 since it should not transmit when N3 is transmitting. This channel selection method is provided until the last destination (i.e., N8)

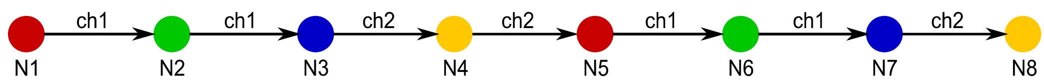

Figure 3-3 Channel selection for long chain topology

Because the network works without a centralized controller, every node will grasp a channel depending on its own activity and condition. As such, the channel selection should be dynamic instead of static. The next section addresses a two channels MAC designed for multihop network with chain and tree topologies.

3.3 THE ALGORITHM OF PROPOSED MAC

In order to achieve a channel selection mechanism as described in Section 3.3, this section will address the algorithm of proposed MAC. Several assumptions accompanying the algorithm are given as follows. In this MAC, each node is equipped with a multichannel transceiver and a simple receiver. The multichannel transceiver is able to receive and send packet through one of two available channels. Meanwhile, the simple receiver can only sense the channel and does not have an ability to receive and decode the packet. The simple receiver will select the channel that is distinct to the channel used by the transceiver. As number of channels considered in this thesis is only two, the simple receiver will be at ch2 if the transceiver is at ch1, and vice versa. With this description, a node works on a half-duplex operation where packet reception cannot be undertaken if the transceiver is transmitting packet. Also, a node will not receive packet at ch1 if its transceiver is operating at ch2, as the simple receiver is not able to receive and process the packet. However, both channels can be sensed at the same time prior to packet transmission as the simple receiver and the receiver of the transceiver are at different channel. With such assumptions, the protocol algorithm is explained as follows.

During packet relaying from a source to the last destination, the transmission channel selection can be different depending on which hop the transmission process is on, as shown in Figure 3-4. If it is the first hop and this is the first packet for this connection, the channel can be chosen randomly. If this is the first hop but not the first packet, the node will try to reuse the channel chosen by the previous packet. If this is in the second hop, the channel chosen by first hop will try to be reused. For the third and subsequent hops, the channel will be assigned by considering the channels utilized in the previous 2 hops.

The algorithm of channel assignment for hop number $n > 2$ is as follows. If the current hop number is n, the channel is chosen by considering the channel used in n-1 and n-2. If hop n-2 uses ch_h (with h can be 1 or 2), and hop n-1 uses ch_i (with i can be 1 or 2), hop n should not choose ch_h to avoid collision with the transmission at hop n-2. Thus, the channel of the next nodes within 2 hops away has been defined before the transmission is undertaken in the current node. Due to this mechanism, the protocol is so called 2 hop channel reservation (2HCR). However, such ideal mechanism can be provided only if all channels are idle. If unfortunately, there is only one available channel, the transmission will be undertaken through this available channel. If both channels are busy, the back off delay will be processed until the available channel(s) are obtained.

```
//Channel selection for hop n of a connection

if (n=1) {                                   //First hop of the connection
       Sense both channels;
       if (Both ch1 and ch2 available) {
               if (this is the first packet)  {
                       Randomly choose one channel;
                       }
               else {
                       Choose the channel used by previous packet;
                       }
               }
        else if (only one channel available) {
               Choose this available channel;
               }
        else {                               //No idle channel
               Back off and try later;
               }
        }

else if (n=2) {                              //Second hop of the connection
        Sense both channels;
        if (both ch1 and ch2 available) {
               Choose the same channel as previous hop;
               }
        else if (only one channel available) {
               Choose this available channel;
               }
        else {
               Back off and try later;
               }
        }

else  {                                      //Third or further hop
       Sense both frequency channels;
       if (both ch1 and ch2 available) {
               Choose the channel different from hop n-2;
               }
       else if (only one channel available) {
               Choose this available channel;
               }
       else {
               Back-off and try later;
               }
        }
```

Figure 3-4 Pseudocode of the proposed 2HCR

The above algorithm could be implemented as a distributed mechanism described as follows. Recalling the topology in Figure 3-3, N1 could choose the channel without dependency to the previous node as it is the source of the packet. N1 then determine the channel should use by N1. To pass this channel information to N2, N1 incorporates the information with the data packet sent to N2. Upon receiving the packet, N2 recognizes the channel suggested by N1 and will use it to forward the packet to N3, if both channels are idle. Prior sending the packet, N2 selects the channel suggested to N3. The channel selection is based on the channel where N2 receives the packet from N1. Once the suggested channel has been determined, N2 includes this information into the packet and send it to N3. The channel selection mechanism undertaken by N2 is also carried out by N3 and the rest of the nodes. This distributed channel selection is depicted in Figure 3-5.

```
//Distributed channel selection mechanism

if (Node is the source) {
        if (This is the first packet)  {
                Randomly choose one channel for its transmission;
                }
        else {
                Choose the channel used by previous packet for its transmission;
                }

        if (The channel is ch1) {
                Suggested transmission channel for the next node is ch1;
                }
        else {                                          // The channel is ch2
                Suggested transmission channel for the next node is ch2;
        }

else if (Node is the last destination) {
        Does need to use the suggested transmission channel;
        Does need to select a suggested transmission channel;
        }

else {                                                  //Relaying node
        Find channel ch_h , where it receives the packet;
        if (ch_h is ch1) {
                Suggested transmission channel for the next node is ch2;
                }
        else {                                          //ch_h is ch2
                Suggested transmission channel for the next node is ch1;
                }
        }
```

Figure 3-5 Distributed channel selection mechanism

As previously mention, the suggested transmission channel is incorporated with the data packet. To do so this channel information could be included as additional bits in the frame body, i.e., payload of the packet frame, or piggybacked in the header of 802.11 MAC [61]. Since the number of channels is only 2, the information can be represented by 1 bit data. 802.11 MAC data frame has a reserved bit that can be utilized to carry the preferred channel information as illustrated in Figure 3-6.

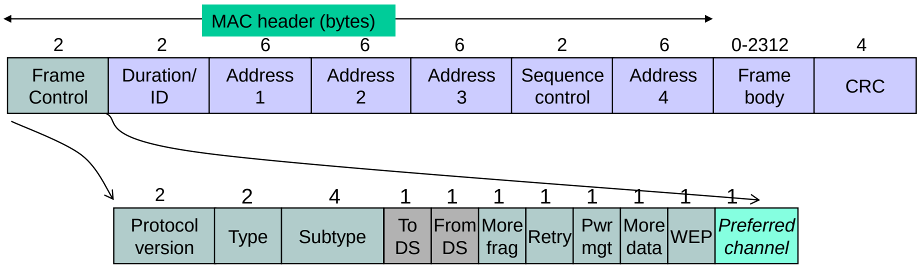

Figure 3-6 The modified 802.11 MAC data frame structure

To examine the performance of 2HCR protocol, simulation is performed through NS3 simulator software [66], in particular with wifi module, which works in 802.11 standard. The wifi module is suitable for simulating an adhoc network as it includes 802.11 MAC DCF protocol that has been used in many studies as discussed in Section 2.3. The simulation will be carried on for 2HCR, and also for 802.11b [61] and MC CSMA [76] to compare their performance. 802.11b is selected as it is generally used in study of multihop network, also representing one channel MAC. Meanwhile, MC CSMA is chosen as it does all channels sense similar with 2HCR.

3.4 SIMULATION PROCEDURE

3.4.1 Simulation Setup

During the simulation, most of parameters are kept in default of NS3 simulator, as long as it is not necessary to set up in a specified value. Generally, the parameters are defined the same to all three protocols, unless the protocol needs to determine its specific parameters. Furthermore, while 2HCR utilizes one transceiver and one simple receiver (as addressed above) as well as MC CSMA, 802.11b protocol utilizes one transceiver. With operation frequency of 2.47 GHz, a channel is set up at ch1, whilst another channel is ch10. The distance between nodes is setup to obtain a situation where a transmitted packet can be received properly by the nodes in 1 hop distance, but not by the nodes in 2 hops distance or beyond.

Furthermore, the bit rate used in the simulation is 1 Mbps, which is the lowest bit rate of 802.11 protocol in wifi module. This data rate is chosen to obtain the longest distance when the system is implemented in the real system. The packet size is fixed with the length of 2000 bits (including MAC and PHY properties). This frame size is able to carry about 8 data packets collected by LH from SNs, which is sent in 25 bytes packet length [92]. By carrying a small number of collected data, a packet frame can be sent immediately without waiting too long for the payload space to be full. For such fixed packet size, the various offered data rate is obtained by setting the average of random interval between packets.

The protocols: 802.11 b, MC CSMA, and 2 HCR are examined under 2 conditions. The first is without RTS/CTS, while another is by activating RTS/CTS. Even though RTS/CTS hand shake is rarely used in a short packet transmission (2000 bits), the simulation is provided to find the network throughput under the influence of RTS/CTS. In addition, although the multihop network is implemented in all tiers, the simulation is provided for tier 2 for simplicity.

3.4.2 Topologies

The performance of the protocols will be evaluated through some topologies that are categorized into 2 topology groups. The first group is the chain topology with 1-source, 2-source and 3-source connected to the edge of the chain topology. 1-source topology is employed as it is used in many studies of multihop network performance. Meanwhile, additional sources, i.e., 2-source and 3-source, are employed to find the effect of multisource to the network performance. A 4-hop version of this type is shown in Figure 3-7. With 4-hop topology, at least 3 pairs of hidden node are configured in the network.

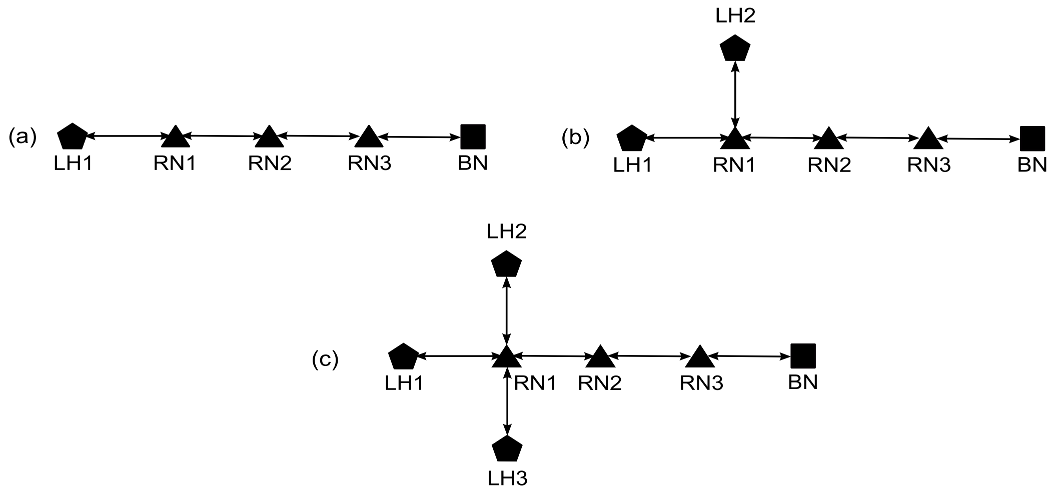

Figure 3-7 4-hop networks with (a) 1-source, (b) 2-source, and (c) 3-source

In a real situation, the hop number can be more than 4 hops due to the longer distance between LH and BN. Therefore, a 7-hop version of this first group is included to examine the effect of higher hop number to the protocol performance. The 7-hop networks with 1-source, 2-source, and 3-source are depicted in Figure 3-8.

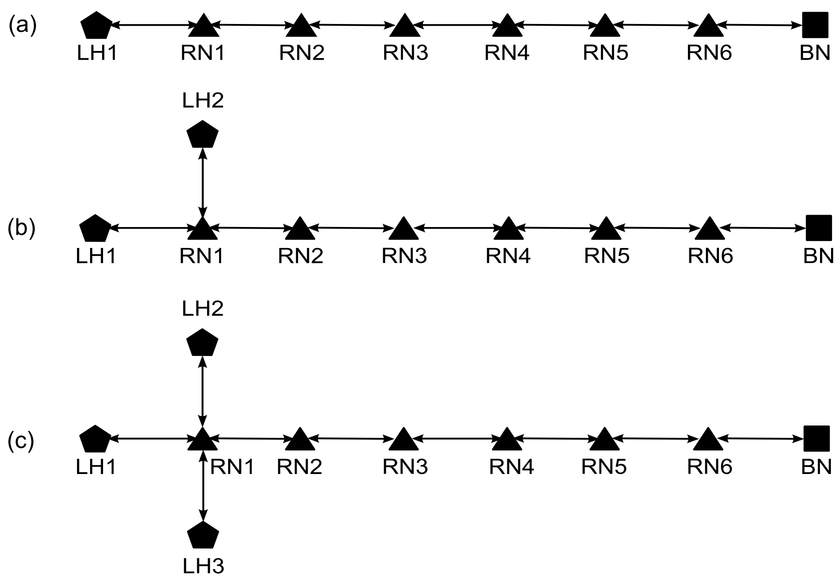

Figure 3-8 7-hop networks with (a) 1-source, (b) 2-source, and (c) 3-source

While in the first topology group, all sources are connected to the edge of the chain (i.e., RN1), in the second group, one of the sources is connected to another RN. This topology is employed to simulate another possible situation in the real network where the sources are not always connected to the same RN. This new branch may affect the traffic flowing from the previous branch/source to the BN. For this group, the number of source is at least 2. For this research, the evaluation utilizes 2-source and 3-source. The 4-hop version of this topology group is depicted in Figure 3-9.

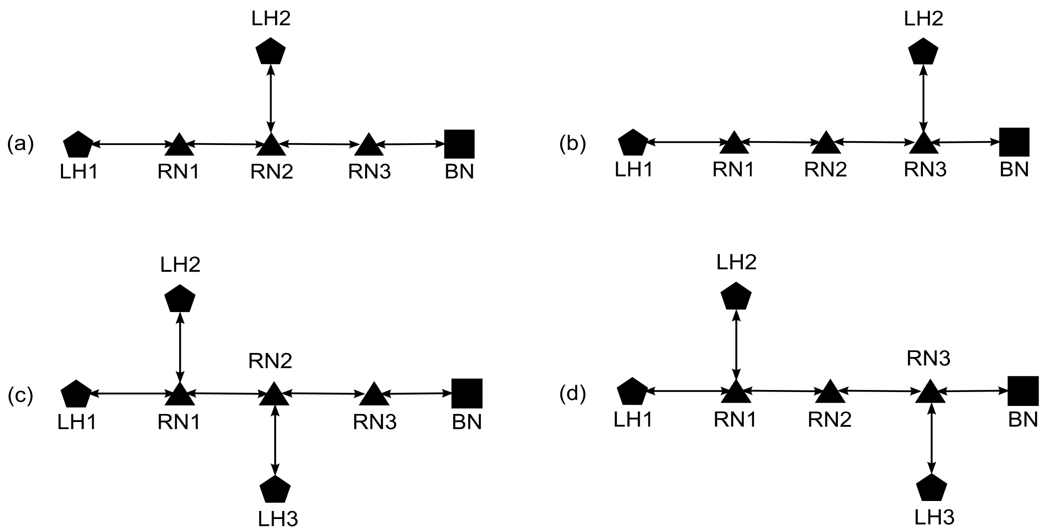

Figure 3-9 4-hop networks with various source location for (a) (b) 2-source, (c) (d) 3-source

Figure 3-9 illustrates the topology of 2-source network with LH2 connected to RN2 (a) or RN3 (b). This distinct connection point is used to observe the effect of different branch location to the packet traffic in the chain. Furthermore, the diagram of 3- source topology with LH3 connected to RN2 is shown in Figure 3-9 (c), while 3-source topology with LH3 connected to RN3 is depicted in Figure 3-9 (d). In addition, as well as in the first group, this second group will also be evaluated in 7-hop version. The topology of 7-hop version is shown in Figure 3-10.

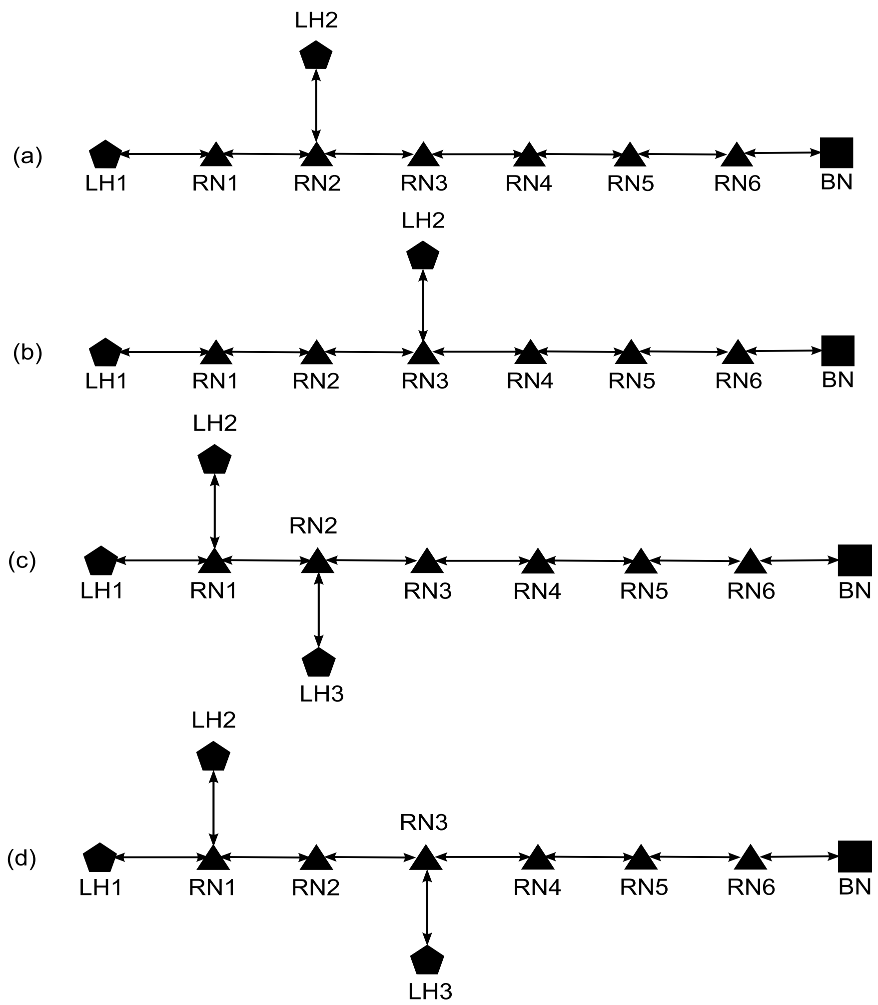

Figure 3-10 7-hop networks with various source location for (a) (b) 2-source, (c) (d) 3-source

3.5 SIMULATION RESULTS AND DISCUSSION

The simulation results of all protocols without activating RTS/CTS handshake are provided in Sections 3.6.1 and 3.6.2. Meanwhile, Section 3.6.3 and 3.6.4 provide the simulation results of all protocols with enabling RTS/CTS. Afterwards, the further discussion of the result is addressed in Section 3.6.5.

3.5.1 Simulation Results of the First Topology Group

The simulation result of 1-source 4-hop is shown in Figure 3-11. For the offered data rate within 100 kbps, the throughputs of all protocols are the same as the offered input rate. The throughput of 802.11b for 100 kbps input rate, however, is less than 100 kbps as it starts to suffer packet loss. The throughput of 802.11b protocol then is saturated at about 135 kbps. This saturation occurs at the input rate of 200 kbps and beyond. On the other hand, the throughput of MC CSMA and 2HCR saturates at the input data rate of 400 kbps and beyond. The maximum throughputs of MC CSMA and 2HCR are 279 kbps, and 289 kbps respectively. It can be seen that 2HCR outperforms 802.11b and MC CSMA protocols.

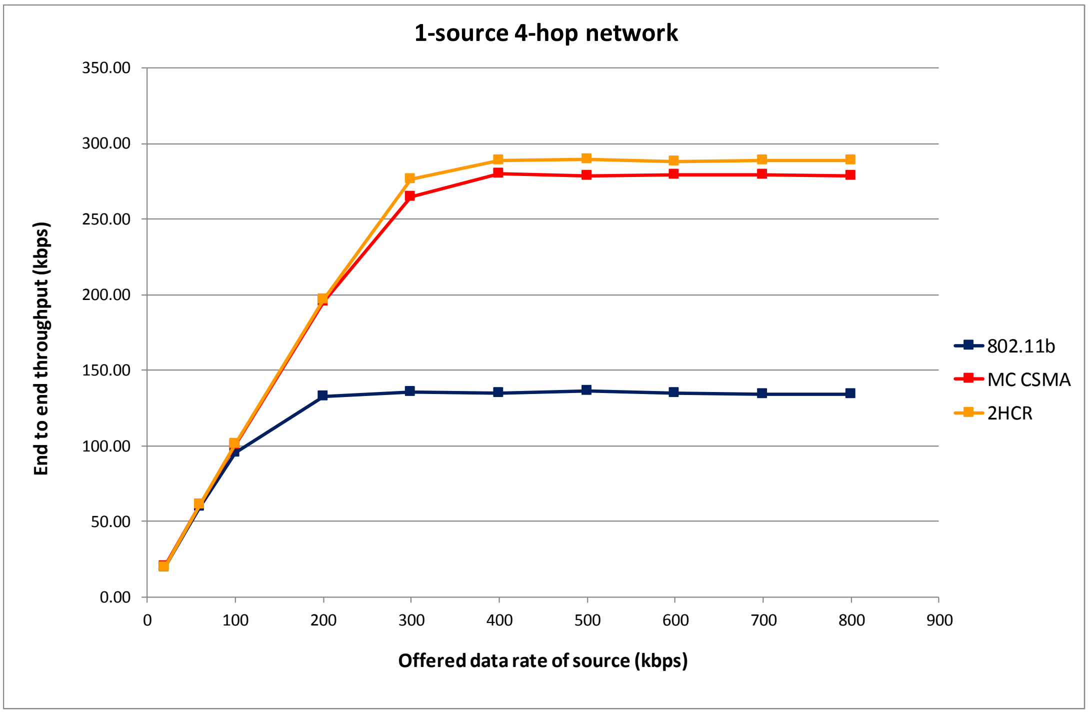

Figure 3-11 The end to end throughput of 1-source 4-hop network

Furthermore, the end to end throughput for 2-source 4-hop network is shown in Figure 3-12. The maximum throughputs of 802.11b, MC CSMA, and 2HCR are 130 kbps, 279 kbps, and 289 kbps respectively. In comparison with 1-source 4-hop, the maximum throughput of 802.11b is decreased by 5 kbps, whereas the throughput of MC CSMA and 2HCR remain constant. The throughput degradation of 802.11 is caused by multisource contention. Meanwhile, the same throughput of 1-source and 2-source in MC CSMA and 2HCR protocol is possibly due to the statistical multisource gain.

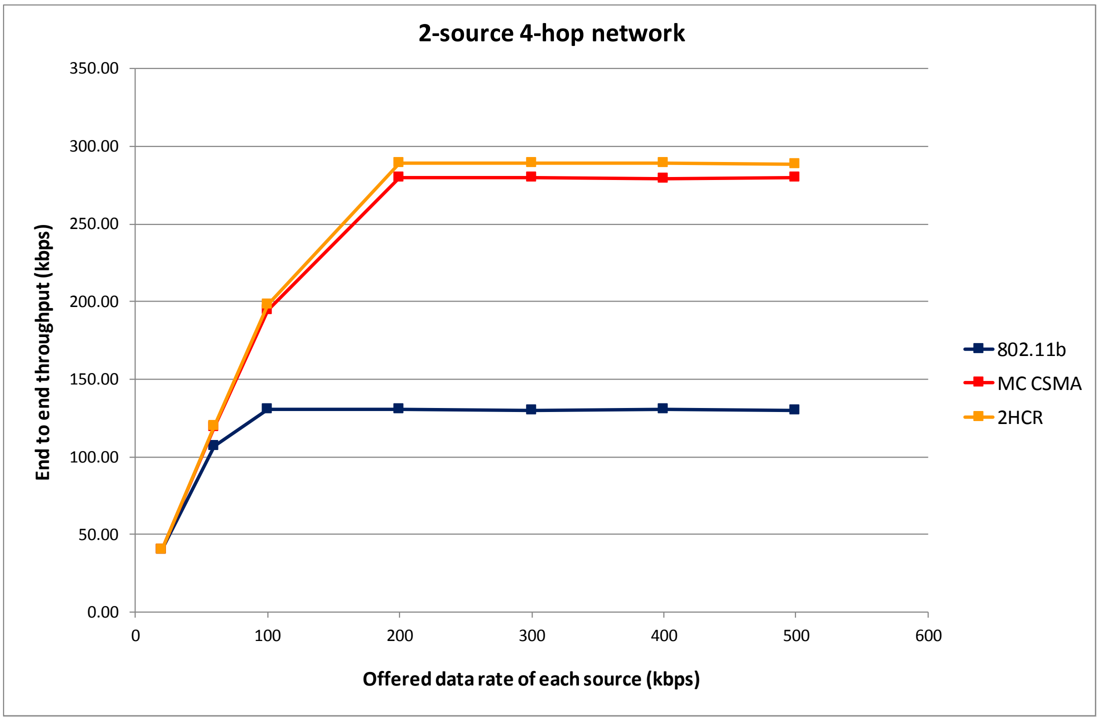

Figure 3-12   The end to end throughput of 2-source 4-hop network

Moreover, the throughput of 3-source 4-hop network is illustrated in Figure 3-13. With one more additional source is connected to RN1, the maximum achievable throughput of 802.11b stays at 130 kbps, which is the same as the throughput of 2-source 4-hop network. It may be because the packets coming from the third source (i.e., LH3) collide with the packets from LH1 and LH2 which are already in collision. On the other hand, the throughputs of MC CSMA and 2HCR are 276 kbps and 286 kbps respectively, which are smaller than in 2-source 4-hop network. It indicates that the packet transmitted by the third source has collided with the packet from either LH1 or LH2.

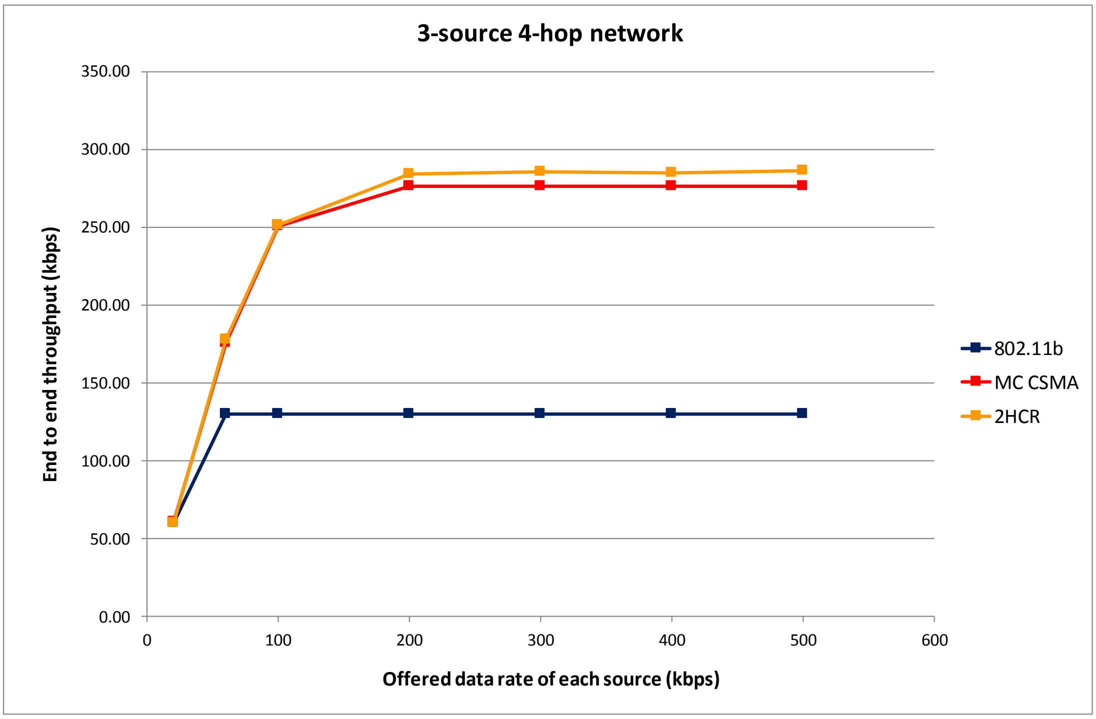

Figure 3-13 The end to end throughput of 3-source 4-hop network

If the maximum achievable throughput obtained by MC CSMA and 2HCR is divided by the maximum throughput of 802.11b protocol, the result, namely the gain over 802.11b, can be tabulated as in Table 3-1. It is shown that the gain of 2HCR in all topologies is higher than the gain of MC CSMA.

Table 3-1 The gain of MC CSMA and 2HCR over 802.11 b for 4-hop network in the first topology group

Number of source	Gain over 802.11 b	
	MC CSMA	2HCR
1-source	2.07	2.14
2-source	2.14	2.22
3-source	2.12	2.20

Meanwhile, the gain of 2-source network is higher than the gain of 1-source network. It is because the throughput of 802.11b protocol is reduced by 5 kbps, whereas the throughput of MC CSMA and 2HCR remains constant. As such the division result of MC CSMA and 2HCR throughputs by 802.11b throughput is higher. Furthermore, even though the throughput of 802.11b protocol for 3-source network remains constant, the throughput of MC CSMA and 2HCR for 3-source network is reduced by 3 kbps. Consequently, the gain of MC CSMA and 2HCR in 3-source network is lower than in 2-source network.

If the hop number is extended into 7-hop network, the throughput of 1-source 7-hop network can be shown in Figure 3-14. Regarding the figure, the maximum throughput of 802.11b, MC CSMA, and 2HCR is 98 kbps, 236 kbps, and 246 kbps respectively. As is expected, the throughputs of all protocols are lower than in 4-hop case due to more hidden and exposed nodes occur in the longer chain. For further comparison, the maximum throughputs of all protocols for 4-hop and 7-hop schemes are gathered in Table 3-2.

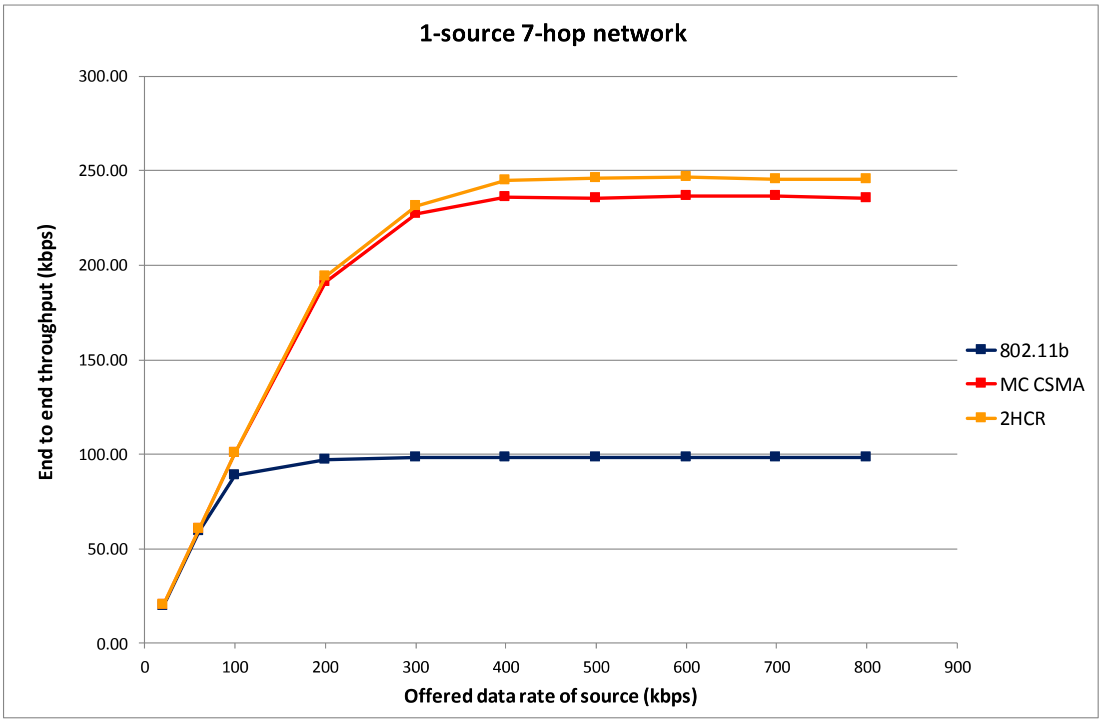

Figure 3-14 The end to end throughput of 1-source 7-hop network

Table 3-2 The maximum throughput of 802.11b, MC CSMA and 2HCR for the first topology group

Hop Number	Number of source	The maximum throughput (kbps)		
		802.11b	MC CSMA	2HCR
4-hop	1-source	135	279	289
	2-source	130	279	289
	3-source	130	276	286
7-hop	1-source	98	236	246
	2-source	89	200	210
	3-source	88	195	209

In general, it is shown that the network throughput decreases when one additional source is included, as number of sources in a connection could lead to multisource contention. The throughput degradation can be various from only 1 kbps, as occurs in 3-source 7-hop 802.11b, to 36 kbps as occurs in 2-source 7-hop MC CSMA. Nevertheless, in some cases, the throughput degradation might not happen possibly due to a statistical multisource gain, as it occurs in 3-source 4-hop 802.11b, 2-source 4-hop MC CSMA, and 2-source 4-hop 2HCR.

To compare the gain of MC CSMA and 2HCR for all topologies in the first group, Table 3-3 denotes the gain obtained from the maximum throughput in Table 3-2. It can be seen that the gain of 2-source network is more less the same as the gain of 3-source network, with the gain of 2HCR is higher than the gain of MC CSMA. However, the gain of 1-source network has different behavior depending on the hop number. In 4-hop network, the gain of 1-source network with both MC CSMA and 2HCR protocols is lower than the gain 2-source and 3-source networks, while in 7-hop, the gain of 1-source network is higher than the gain of 2-source and 3-source networks, and even achieves the highest gain among the other topologies. According to the maximum throughput in Table 3-2, it might be due to 27.47 %

throughput degradation from 4-hop to 7-hop which is suffered by 802.11b protocol, while MC CSMA and 2HCR suffer only 15.41 % and 14.88 % respectively.

Table 3-3 The gain of MC CSMA and 2HCR over 802.11 b
for the first topology group

Number of hop	Number of source	Gain over 802.11 b	
		MC CSMA	2HCR
4-hop	1-source	2.07	2.14
	2-source	2.14	2.22
	3-source	2.12	2.20
7-hop	1-source	2.41	2.51
	2-source	2.25	2.36
	3-source	2.22	2.38

3.5.2 Simulation Results of the Second Topology Group

The throughput of 2-source 4-hop network with 2 different locations of LH2 is shown in Figure 3-15. The solid line represents the throughput if LH2 is connected to RN2 as shown in Figure 3-10 (a). Concurrently, the dotted line indicates the throughput if LH2 is connected to RN3 as shown in Figure 3-10 (b). Regarding the graphs of the earlier topology, the throughputs of 802.11b, MC CSMA, and 2HCR are 180 kbps, 320 kbps, and 330 kbps respectively. Such throughputs are higher than the throughputs of 2-source 4-hop topology in the first group. As such, it gives evidence that LH2 connection movement from RN1 to RN2, which is closer to the destination BN, can elevate the throughput as the hop number to reach BN is declined. Further movement by connecting LH2 with RN3, even gives the higher throughputs with 302 kbps, 468 kbps, and 482 kbps for 802.11b, MC CSMA, and 2HCR respectively. These throughputs are almost two times than the throughputs of 2-source 4-hop in the first topology group.

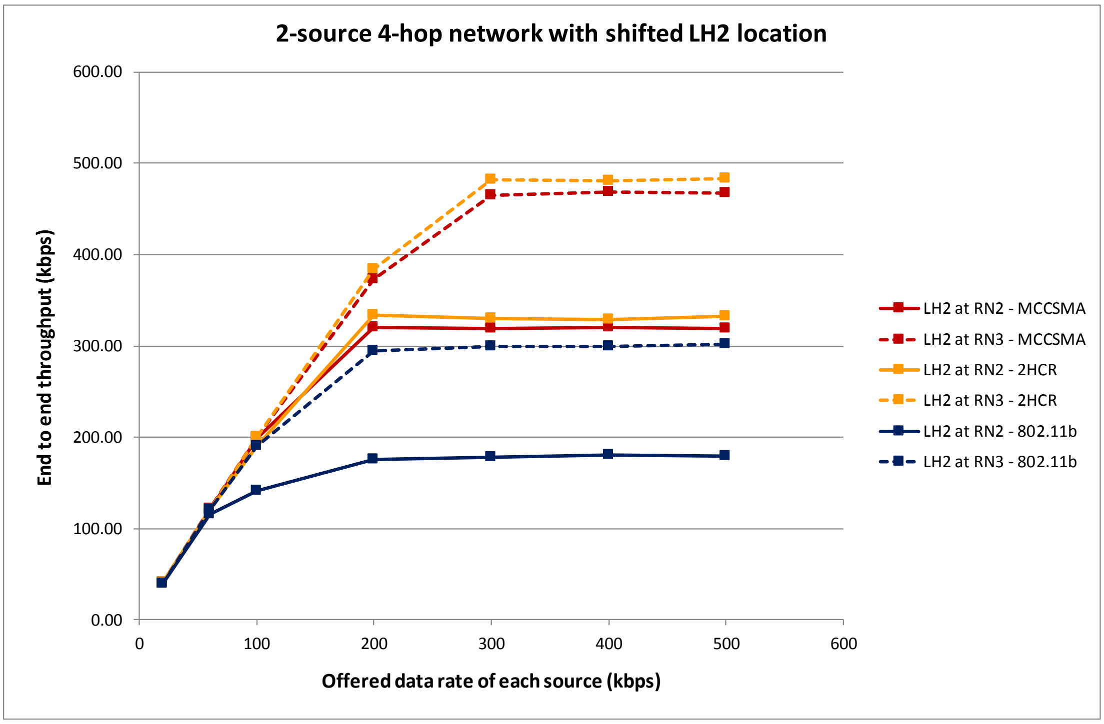

Figure 3-15 The end to end throughput of 2-source 4-hop networks with shifted LH2 location

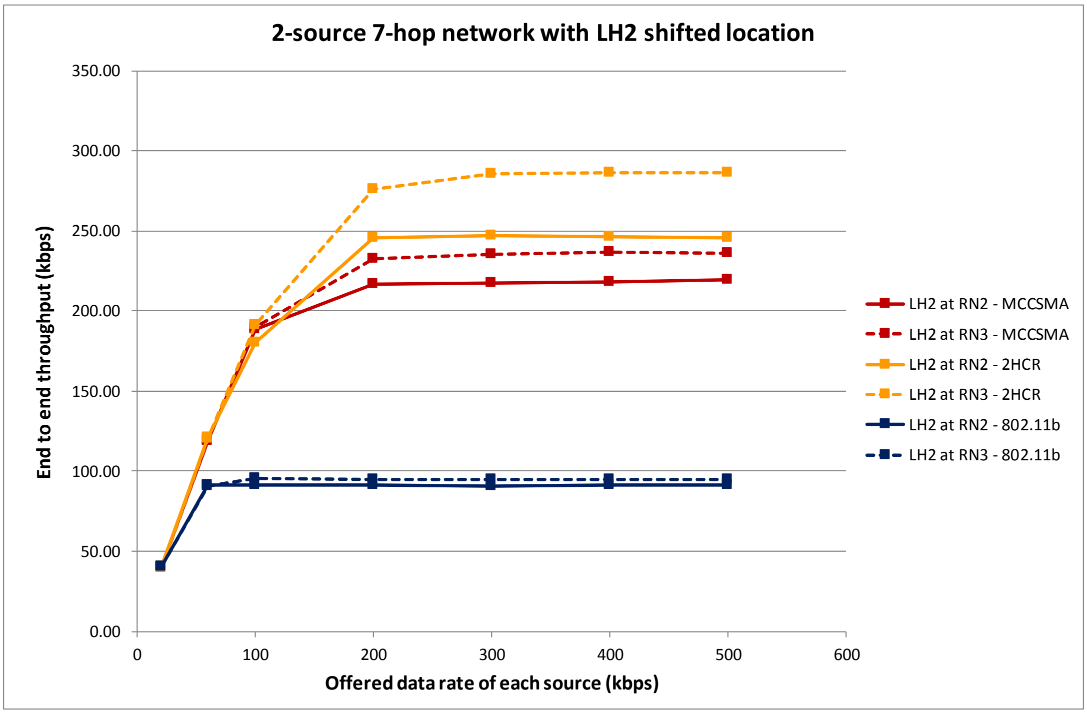

Figure 3-16 The end to end throughput of 2-source 7-hop networks with shifted LH2 location

On the other hand, the throughput of the 2-source 7-hop network with LH2 connected to RN2 (Figure 3-10 (a)) and LH2 connected to RN3 (Figure 3-10 (b)) is depicted in Figure 3-16. The solid curves denote that the maximum throughputs of 802.11b, MC CSMA, and 2HCR for the earlier topology are 91 kbps, 219 kbps, and 247 kbps respectively. Compared to 4-hop scenario with the same topology, these maximum throughputs are lower. The same throughput declination is also suffered by the later topology, with the maximum throughput of 802.11b achieves 94 kbps, MC CSMA achieves 237 kbps, and 2HCR obtains 286 kbps. However, the comparison between these two topologies of 7-hop network, again shows that the maximum achievable throughput of network with LH2 connected to RN3 is higher than LH2 connected to RN2 as well as in 4-hop networks.

By means of the throughput yielded from the simulation, the gain of the three protocols for 2-source network in the second topology group can be tabulated as shown in Table 3-4. It can be seen that the gain of 7-hop network is higher than the gain of 4-hop network. As obtained in the first topology group, the higher gain of 7-hop network is caused by the higher throughput degradation in 802.11b compared to MC CSMA and 2HCR. The smallest degradation in 802.11b achieved by 2-source 7-hop network with LH2 connected to RN3, is 49.44 %. On the other hand, the highest degradation of MC CSMA and 2HCR is only 49.36 % and 40.66 % respectively. By the way, the gain of 2HCR outperforms the gain of MC CSMA in all topologies.

Table 3-4 The gain of MC CSMA and 2HCR over 802.11 b for the 2-source network in the second topology group

Number of hop	LH2 connection	Gain over 802.11b	
		MC CSMA	2HCR
4-hop	at RN2	1.78	1.83
	at RN3	1.55	1.60
7-hop	at RN2	2.41	2.71
	at RN3	2.52	3.04

Meanwhile, the simulation results for 3-source 4-hop topologies depicted in Figure 3-9 (c), (d) and 3-source 7-hop topologies depicted in Figure 3-10 (c), (d) are tabulated in Table 3-5. It can be seen that the maximum throughput of network with LH3 is connected to RN3 is higher than the maximum throughput of network with LH3 is connected to RN2. It denotes that the closer connection to BN can allow LH3 to send much more packets. Also, it is denoted that the throughput of 7-hop is lower than in 4-hop due to more collisions occurred by more hidden nodes in the longer chain.

Table 3-5 The maximum throughput of 802.11 b, MC CSMA and 2HCR for the 3-source network in the second topology group

Number of hop	LH3 connection	Maximum throughput (kbps)		
		802.11b	MC CSMA	2HCR
4-hop	at RN2	149	277	300
	at RN3	294	452	496
7-hop	at RN2	89	215	254
	at RN3	93	233	278

For the given throughputs in Table 3-5, the gains of MC CSMA and 2HCR over 802.11b are obtained as tabulated in Table 3-6. It shows the gain of MC CSMA and 2HCR in 7-hop is higher than in 4-hop scheme, as obtained by the first topology group. This is because 802.11b protocol in these topologies also suffer the higher throughput degradation than MC CSMA and 2HCR. By the way, the gain of 2HCR is higher than MC CSMA in all topologies.

Table 3-6 The gain of MC CSMA and 2HCR over 802.11 b for the 3-source network in the second topology group

Number of hop	LH3 connection	Gain over 802.11b	
		MC CSMA	2HCR
4-hop	at RN2	1.86	2.01
	at RN3	1.54	1.69
7-hop	at RN2	2.42	2.85
	at RN3	2.51	2.99

3.5.3 Simulation Results of the First Topology Group with Protocol Enabling RTS/CTS

The simulation results in Section 3.6.1 have presented how the number of hop, and the number of source can affect the end to end throughput of the network. All such simulations show the performance of the protocol 802.11b, MC CSMA, and 2HCR without involving RTS/CTS handshake. In this section, the performance of the three protocols is evaluated under condition where RTS/CTS handshake is utilized by all protocols. For 1-source 4-hop network, the end to end throughput of 802.11b, MC CSMA, and 2HCR is shown in Figure 3-17.

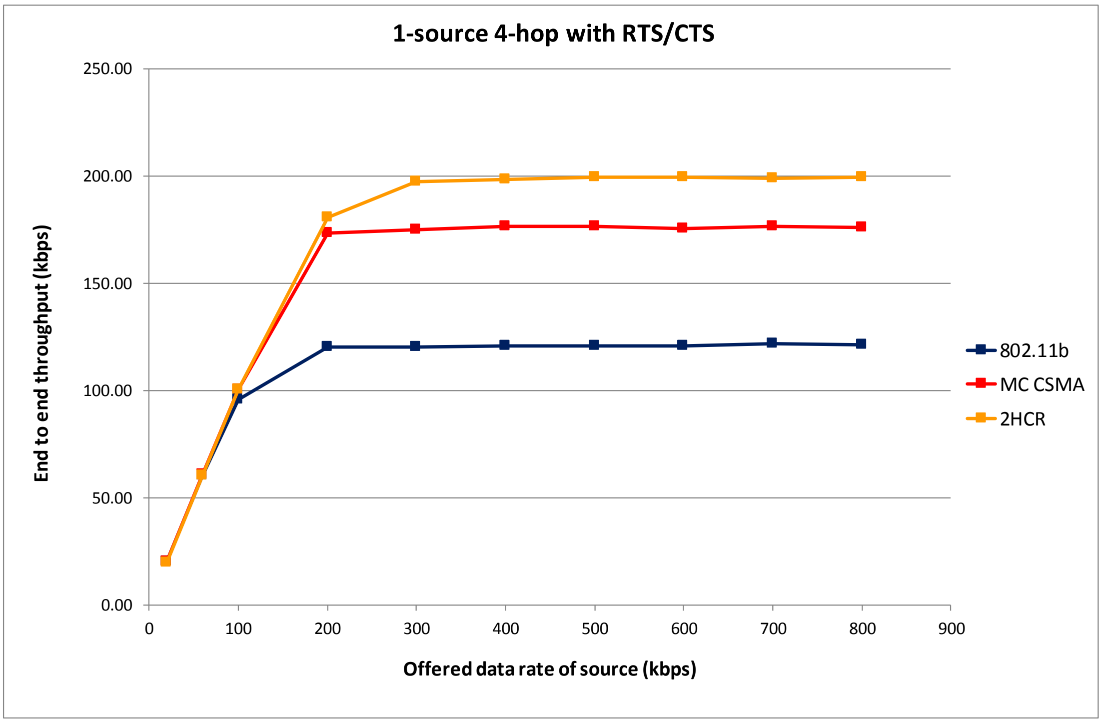

Figure 3-17 The end to end throughput of 1-source 4-hop network with protocol enabling RTS/CTS

According Figure 3-17, for the input data rate of 20 kbps to 100 kbps the throughput of all protocols is similar with the respected input data rate. Afterwards, the throughput of 802.11b and MC CSMA is saturated starting at the input data rate of 200 kbps, whereas the throughput of 2HCR has just saturated at the input data rate of 300 kbps. The throughputs of 802.11b, MC CSMA, and 2HCR protocol are maximum at 121 kbps, 177 kbps, and 199 kbps respectively.

Compared to the maximum throughput for the same topology in Section 3.6.1 i.e., without RTS/CTS, the maximum throughput with protocol enabling RTS/CTS is lower. This is due to the inclusion of RTS and CTS packets that increase the contention already happen between data packets, particularly at the high input data rate where the interval between data packet is small. As such, a number of successful data packets delivered to the destination is smaller. For the input data rate of 20 kbps and 60 kbps, which is relatively low, it may only a small number of RTS/CTS packets colliding with the data packet as the interval between data packet is large. Therefore, although RTS/CTS handshake can improve the throughput of multihop network by minimizing the effect of hidden node problem, the use of RTS/CTS for a short packet could become a costly overhead as has been investigated in [23].

Furthermore, the simulation result of 2-source 4-hop network is shown in Figure 3-18. The maximum throughputs of 802.11b, MC CSMA, and 2HCR protocols are 128 kbps, 175 kbps, and 189 kbps respectively. These throughputs are smaller than the throughputs of the same topology with the protocol disabling RTS/CTS in Section 3.6.1. Again, as explained in the previous paragraph, the lower throughput is due to the employment of RTS/CTS packets that reduces the opportunity of successful data packet delivery.

On the other hand, in comparison with the result in 1-source topology, the throughput of MC CSMA and 2HCR of 2-source topology is lower. It indicates that the collision is also caused by multisource contention. However, the throughput of 802.11b is surprisingly 7 kbps higher than in 1-source 4-hop topology. It is more likely caused by the statistical multiplexing gain of multisource.

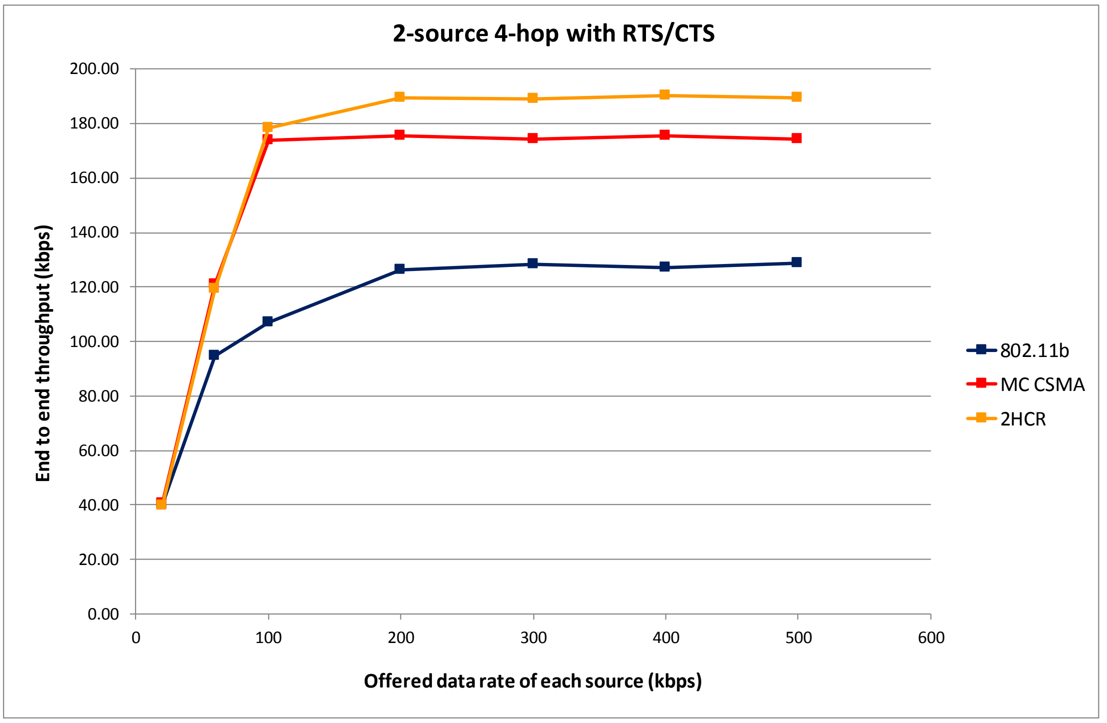

Figure 3-18 The end to end throughput of 2-source 4-hop network with protocol enabling RTS/CTS

Moreover, the simulation result of 3-source 4-hop network is shown in Figure 3-19. The maximum achievable throughputs of 802.11b, MC CSMA, and 2HCR are 126 kbps, 168 kbps, and 180 kbps respectively. Similar with the previous 1-source and 2-source networks, the throughputs in this scenario are smaller than the throughputs of the same network with protocol disabling RTS/CTS as explained in Section 3.6.1. Concurrently, in comparison with the previous 2-source network, the maximum throughput of 3-source 4-hop network is smaller. Thus, the throughput degradation due to multisource contention also happens in this scenario.

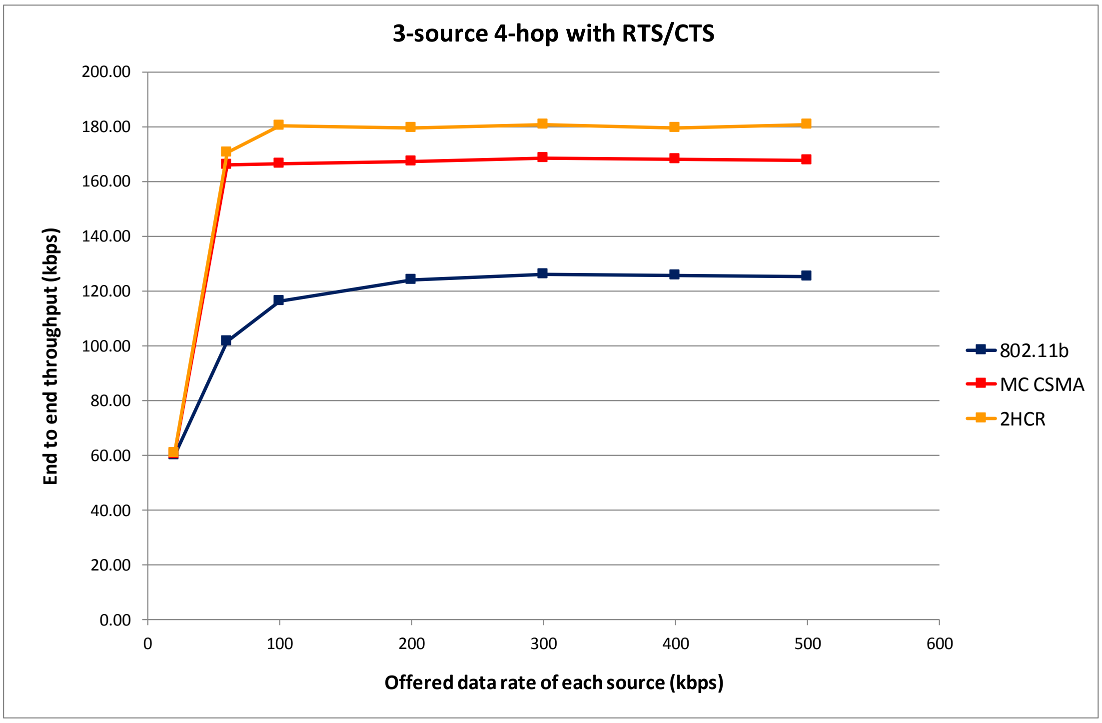

Figure 3-19 The end to end throughput of 3-source 4-hop network with protocol enabling RTS/CTS

Similar with the first topology group, the maximum throughput of MC CSMA and 2HCR can be divided by the maximum throughput of 802.11b protocol to obtain the gain over 802.11b. The gain of MC CSMA and 2HCR for 4-hop network with various numbers of sources is tabulated in Table 3-7.

Table 3-7 The gain of MC CSMA and 2HCR over 802.11b for 4-hop network with enabled RTS/CTS in the first topology group

Number of source	Gain over 802.11b	
	MC CSMA	2HCR
1-source	1.46	1.65
2-source	1.37	1.48
3-source	1.33	1.43

In comparison with the result of disabled RTS/CTS protocol in Table 3-1, the gain over 802.11b in Table 3-7 is lower. The reason is because the throughput degradation suffered by 802.11b in applying RTS/CTS is lower than it is suffered by MC CSMA and 2HCR. The throughput degradation of 802.11b for all topologies in the first topology group is less than 10%, whilst MC CSMA and 2HCR suffer the throughput degradation higher than 30 %. Thus, a division to calculate the gain is lower than in Table 3-1.

If the chain of the network is extended into 7-hop, the throughput of 1-source 7-hop network can be depicted as in Figure 3-20. The maximum achievable throughput of 802.11b is 86 kbps, MC CSMA is 134 kbps, and 2HCR is 143 kbps. Similar with the throughputs of RTS/CTS disabled protocol in Section 3.6.1, the throughputs of all protocols decline when the chain length is extended.

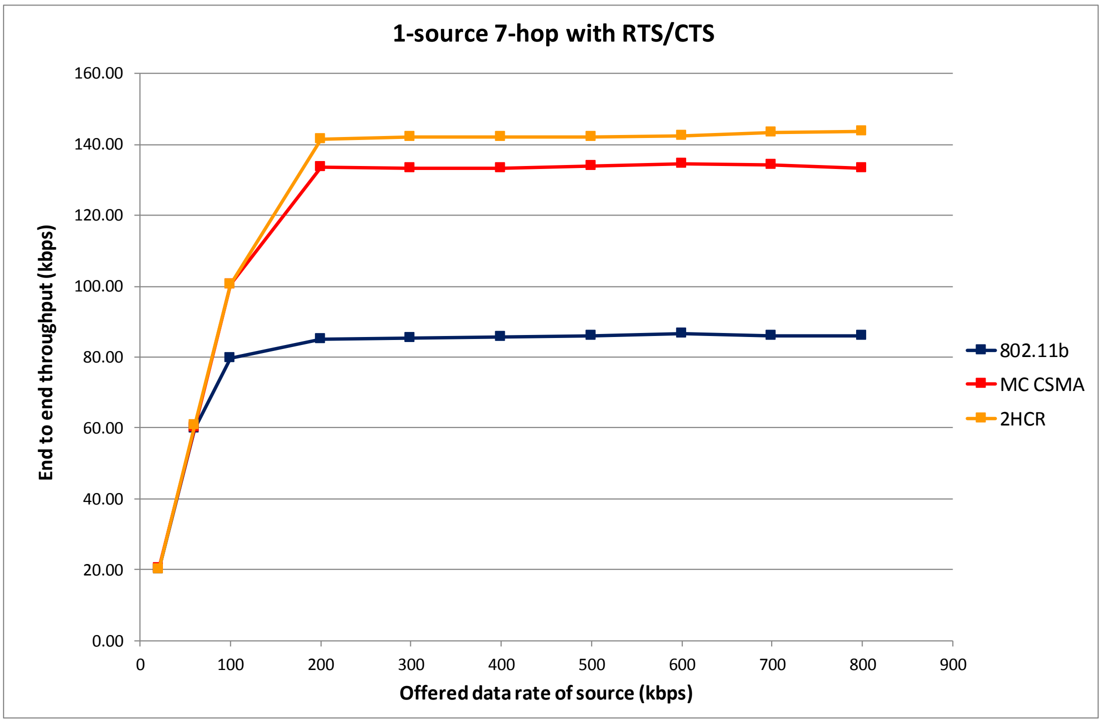

Figure 3-20 The end to end throughput of 1-source 7-hop network with protocol enabling RTS/CTS

To observe the throughputs of 2-source 7-hop and 3-source 7-hop, the results are collected in Table 3-8. Such table also gathers the maximum throughputs of 4-hop network for further comparison.

Table 3-8 The maximum throughput of 802.11 b, MC CSMA and 2HCR with enabled RTS/CTS for the first topology group

Hop Number	Number of source	The maximum throughput (kbps)		
		802.11b	MC CSMA	2HCR
4-hop	1-source	121	177	199
	2-source	128	175	189
	3-source	126	168	180
7-hop	1-source	86	134	143
	2-source	86	125	127
	3-source	84	123	125

As the hop number grows up, the throughputs of all protocols decline. The throughputs also degrade when the number of source is increased. A different trend, however, is obtained in 802.11b with 2-source 4-hop, and 2-source 7-hop. The throughput of 2-source 4-hop is higher than 1-source 4-hop. The possible explanation is due to the multisource statistical multiplexing gain as has been mentioned in previous discussion of the first topology in Subsection 3.6.1. Similarly, the same throughput obtained by 2-source 7-hop and 1-source 7-hop is possibly due to a statistical multisource gain.

Furthermore, the gain of MC CSMA and 2HCR over 802.11b of all topologies in Table 3-8 is denoted in Table 3-9. It is shown that generally the gain of 7-hop network is higher than 4-hop, excepted for 1-source 7-hop with 2HCR protocol. The high gain performed by 2HCR at 1-source 4-hop topology could be due to the high performance of 2HCR at this topology.

Table 3-9 The gain of MC CSMA and 2HCR over 802.11 b with enabled RTS/CTS for the first topology group

Number of hop	Number of source	Gain over 802.11 b	
		MC CSMA	2HCR
4-hop	1-source	1.46	1.79
	2-source	1.37	1.48
	3-source	1.33	1.43
7-hop	1-source	1.56	1.66
	2-source	1.45	1.48
	3-source	1.46	1.49

3.5.4 Simulation Results for The Second Topology Group with Protocol Enabling RTS/CTS

Figure 3-21 illustrates the throughput of 2-source 4-hop topology with LH2 is connected to either RN2 as depicted in Figure 3-9 (a), or RN3 as depicted in Figure 3-9 (b). The throughput of the earlier is represented by the solid line, while the later is represented by dotted line. Regarding the curves with the solid line, the maximum throughputs of 802.11b, MC CSMA, and 2HCR are 131 kbps, 256 kbps, and 262 kbps respectively. In comparison with the maximum throughput of 2-source 4-hop network in the first topology group, these throughputs are higher. Therefore, the shifted connection of LH2 to RN2 has increased the maximum throughput as the hop number between LH2 and BN is declined. The further increase is obtained when LH2 is connected to RN3. In this case, the maximum achievable throughput of 802.11b is 255 kbps, MC CSMA is 438 kbps, and 2HCR is 443 kbps.

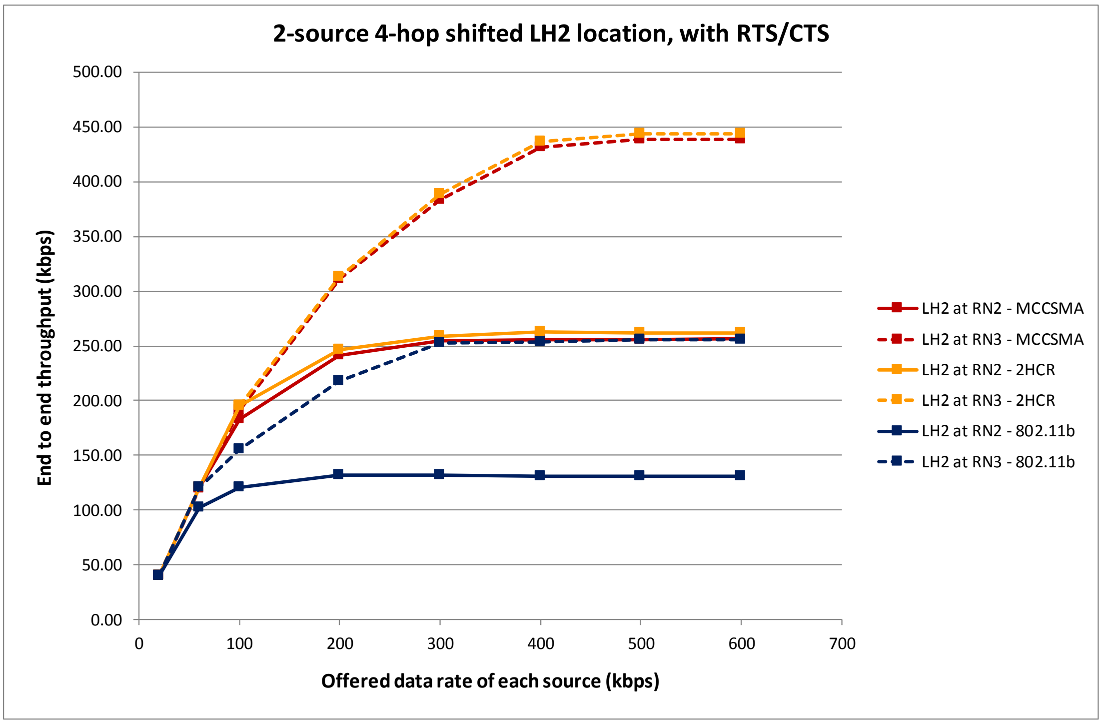

Figure 3-21 The end to end throughput of 2-source 4-hop network with shifted LH2 location and enabled RTS/CTS protocols

If the network chain is extended to 7-hop, the maximum achievable throughputs of 802.11b, MC CSMA, and 2HCR in 2-source 7-hop network with LH2 connected to RN2, reach 80 kbps, 139 kbps, and 142 kbps respectively, as depicted in Figure 3-22. These throughputs are smaller than in 4-hop network. Meanwhile, when LH2 is connected to RN3, the maximum throughput of 802.11b achieves 82 kbps, MC CSMA achieves 160 kbps, and 2HCR achieves 169 kbps. These throughputs are also smaller than in 4-hop network. Furthermore, if the throughput of these different topologies is compared, the throughput of network with LH2 is connected to RN3 is higher than the throughput of network with LH2 is connected to RN2. The smaller hop number of LH to BN, again becomes the reason for LH2 to send more successful packets.

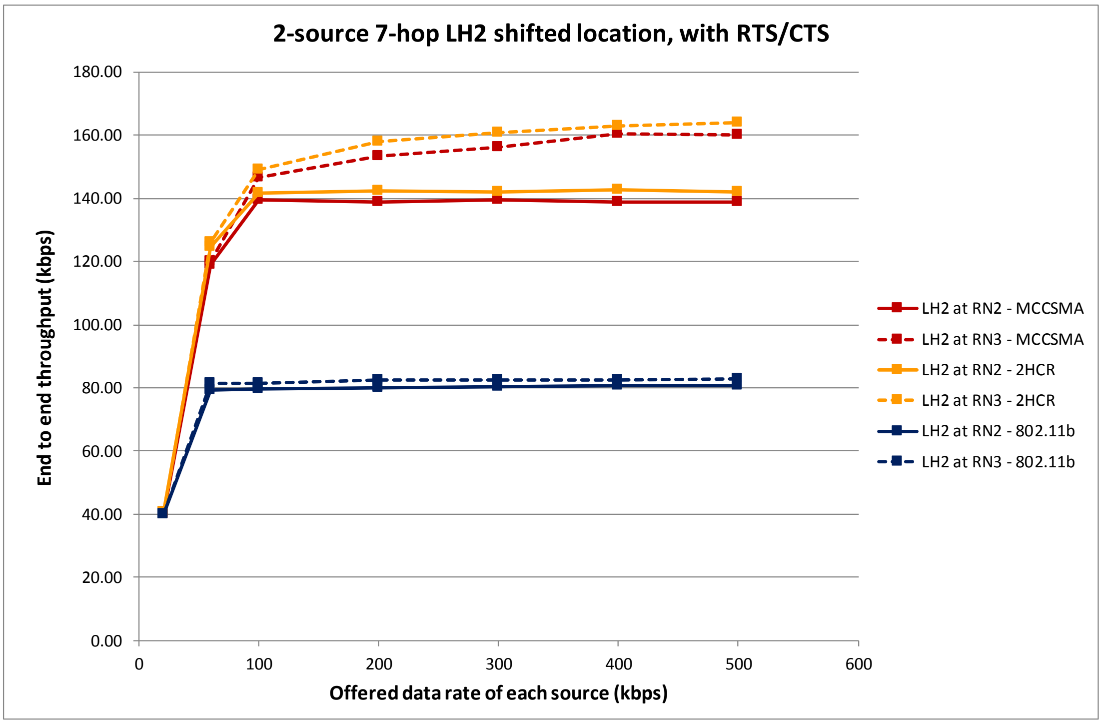

Figure 3-22 The end to end throughput of 2-source 7-hop network with shifted LH2 location and enabled RTS/CTS protocols

Based on the throughputs obtained from the simulation, the gain of MC CSMA and 2HCR over 802.11b can be calculated, with the results are tabulated in Table 3-10. For the topology where LH2 is connected to RN3, the gain in 7-hop network is higher than in 4-hop network. However, for the network with LH2 connected to RN2, the gain in 7-hop network is smaller than in 4-hop network. This result does not follow the trend that matches with all previous simulations. The possible reason is because MC CSMA and 2HCR suffer the higher throughput degradation than 802.11b. The degradation of MC CSMA and 2HCR reach 45.70 % and 45.80 %, whereas 802.11b suffers only 38.93 %. Furthermore, the gain of 2HCR outperforms the gain of MC CSMA in all topologies.

Table 3-10 The gain of MC CSMA and 2HCR over 802.11 b for 2-source network in the second topology with shifted LH2 location and enabled RTS/CTS protocols

Number of hop	LH2 Connection	Gain over 802.11b	
		MC CSMA	2HCR
4-hop	at RN2	1.96	2.00
	at RN3	1.72	1.74
7-hop	at RN2	1.74	1.78
	at RN3	1.95	2.06

Concurrently, the maximum throughputs of the three protocols in 3-source networks are collected in Table 3-11. Following the trend in previous simulations, the throughputs of all protocols increase when the connection of LH3 is moved from RN2 to RN3. In addition, 2HCR performance is always better than MC CSMA and 802.11b.

Table 3-11 The maximum throughput of 802.11b, MC CSMA and 2HCR for 3-source network in the second topology with shifted LH3 location and enabled RTS/CTS protocols

Number of hop	LH3 Connection	Maximum throughput (kbps)		
		802.11b	MC CSMA	2HCR
4-hop	at RN2	126	235	239
	at RN3	257	451	464
7-hop	at RN2	80	144	150
	at RN3	82	168	173

For the given maximum throughput, the gain of MC CSMA and 2HCR over 802.11b performance is gathered in Table 3-12. When LH3 is connected to RN3, the gains of MC CSMA and 2HCR in 7-hop network are higher than in 4-hop. This matches with the trend of the most results. However, if LH3 is connected to RN2, the extension of hop number from 4-hop to 7-hop leads to the small gain degradation. These distinct results occur as the throughput degradations of MC

CSMA, i.e., 38.72 %, and 2HCR, i.e., 37.24 %, from 4-hop to 7-hop are higher than 802.11b, i.e., 36.51 %. As such, the division to yield the gain obtains the small value.

Table 3-12 The gain of MC CSMA and 2HCR over 802.11b for 3-source network in the second topology with shifted LH3 location and enabled RTS/CTS protocols

Number of hop	LH3 Connection	Gain over 802.11b	
		MC CSMA	2HCR
4-hop	at RN2	1.87	1.90
	at RN3	1.76	1.81
7-hop	at RN2	1.80	1.88
	at RN3	2.05	2.11

3.5.5 Discussion

During the performance evaluation through various topologies, 2HCR has proven outperforming MC CSMA in all topologies. However, the comparison between 2HCR and MC CSMA shows that in several topologies, the performance of 2HCR is significantly higher than MC CSMA, as indicated by the gain over 802.11b throughput. It denotes that 2HCR has more advantage when it is implemented in specific topologies. To find such advantage, the mechanism of 2HCR protocol is required to compare with the mechanism of MC CSMA protocol.

Albeit MC CSMA and 2HCR utilize the same number of channel (i.e., 2 channels in this case), the way to select the channel is different. In MC CSMA, if the protocol finds that all channels are idle, the transmission channel will be chosen randomly. On the other hand, 2HCR chooses the transmission channel by considering the channel utilization of previous RNs within 2 hops away. As 2HCR defines the transmission channel of every three consecutive RNs, the collision caused by hidden node could be significantly reduced compared to MC CSMA that the transmission channel of a node is defined by this node individually. With such mechanism, 2HCR can have a better channel use distribution.

Furthermore, when both channels are busy, MC CSMA and 2HCR will re-sense the channel. However, MC CSMA and 2HCR have the different way in choosing which channel is being waited to be idle. MC CSMA prefers to wait the first channel to be idle, whilst 2HCR waits for any channel to be idle. Consequently, 2HCR can have a shorter time in executing the transmission over MC CSMA.

To further examine the effect of such different mechanism, the measurement of channel selection is undertaken for 2 topologies. One topology is chosen as the difference between the gain obtained by 2HCR and MC CSMA is small, whereas another topology is chosen as the difference between the gain obtained by 2HCR and MC CSMA is big. For the first case, 2-source 7-hop network in the first topology group is selected as the difference between the gain obtained by 2HCR and MC CSMA is only 0.11. In this case, 2HCR yields the gain of 2.36 whereas MC CSMA obtains 2.25. Meanwhile, 2-source 7-hop network with LH2 connected to RN3 is chosen for the second case as the difference between the gain yielded by 2HCR and MC CSMA is 0.52. In this case, 2HCR obtains 3.04, while MC CSMA obtains 2.52.

To measure the channel utilization, the simulation time is set for 100 seconds measurement period, with sources LH1 and LH2 generate 500 kbps data rate. The simulation will display how many times a channel is used for the packet transmission, including retransmission. As such, the counter does not represent the number of successful packet transmission.

For 2-source 7-hop of the first topology group, the channel assignment of MC CSMA is denoted in Figure 3-23. It can be seen that MC CSMA in most of RNs refers to use ch1 rather than ch2. It is appropriate with the protocol mechanism where ch1 is preferred to be waited when both channels are busy. Consequently, collision may occur when two nodes separated 2 hop away transmit at the same time.

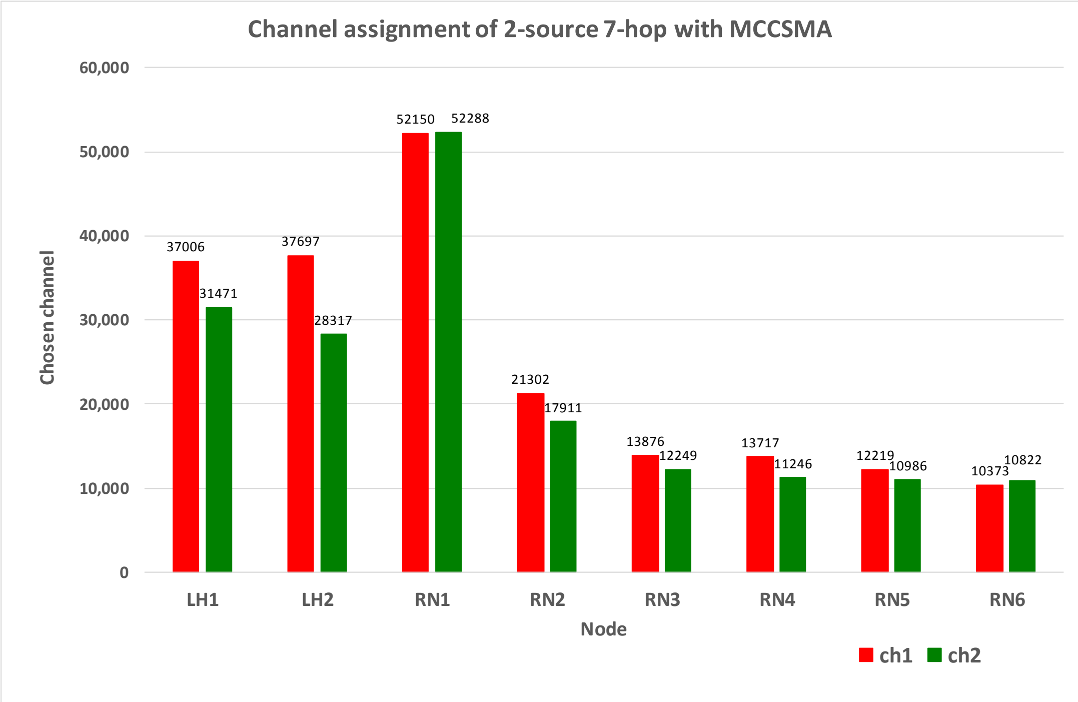

Figure 3-23 The channel assignment of MC CSMA in 2-source 7-hop network

The channel selection of 2HCR in 2-source 7-hop network in the first group is shown in Figure 3-24. Unlike MC CSMA, the chosen channel in 2HCR is distributed similarly to ch1 and ch2. Furthermore, with the preferred channel configuration following the pattern of ch1-ch1-ch2-ch2-ch1-ch1-ch2 as intended by 2HCR (discussed in Section 3.3), the collision between 2 nodes separated 2 hops away can be reduced. This comparison gives the explanation how 2HCR overcoming the performance of MC CSMA.

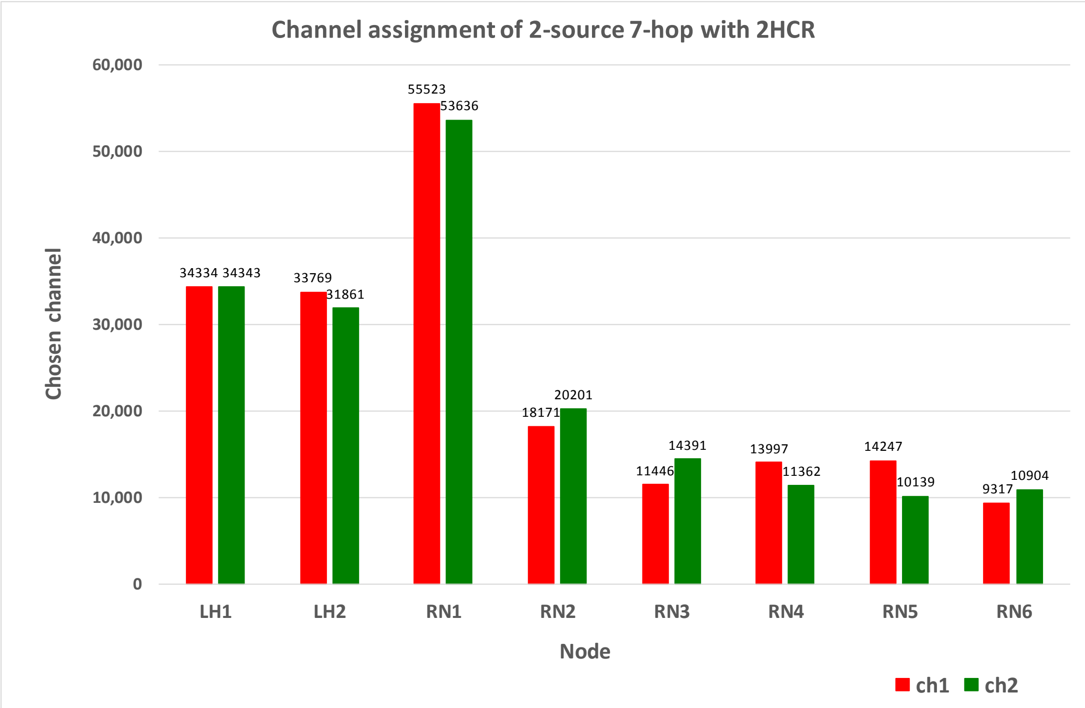

Figure 3-24 The channel assignment of 2HCR in 2-source 7-hop network

Further observation of the effect of channel selection throughout the network, can be carried on by using Figure 3-25, which illustrates the configuration of the preferred channel obtained from Figure 3-23 and 3-24. Despite it is certain that collision possibly occurs at all nodes, the channel selection pattern can indicate in which node the collision occurs more likely.

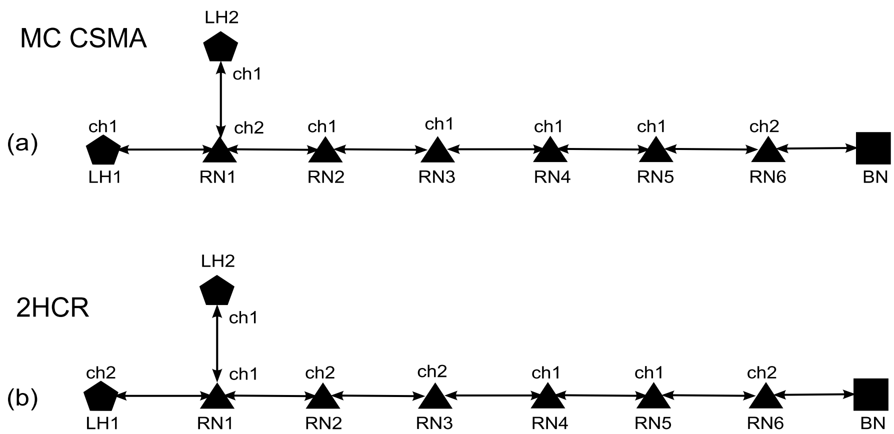

Figure 3-25 The channel assignment configuration in 2-source 7-hop network for (a) MC CSMA and (b) 2HCR

According Figure 3-25 (a), the collision in MC CSMA mostly happens at RN1, RN3, and RN4 as surrounding nodes prefer to transmit at the same channel, i.e., ch1. Compared to RN3 and RN4 that have 2 neighbours to contend the channel, RN1 suffers more collision since the same channel is contended by three neighbour nodes (LH1, LH2, and RN2). On the other hand, according Figure 3-25 (b), the collision in 2HCR mostly occurs at only RN1 as LH1 and RN2 have the same preferred channel. For the other nodes, the collision could be reduced as the preferred channel configuration follows the pattern intended by 2HCR protocol.

Furthermore, Figure 3-26 illustrates the channel preference of MC CSMA for 2-source 7-hop network with LH2 connected to RN3. It can be seen that ch1 is preferred to use rather than ch2. Consequently, the channel contention happens throughout the entire network.

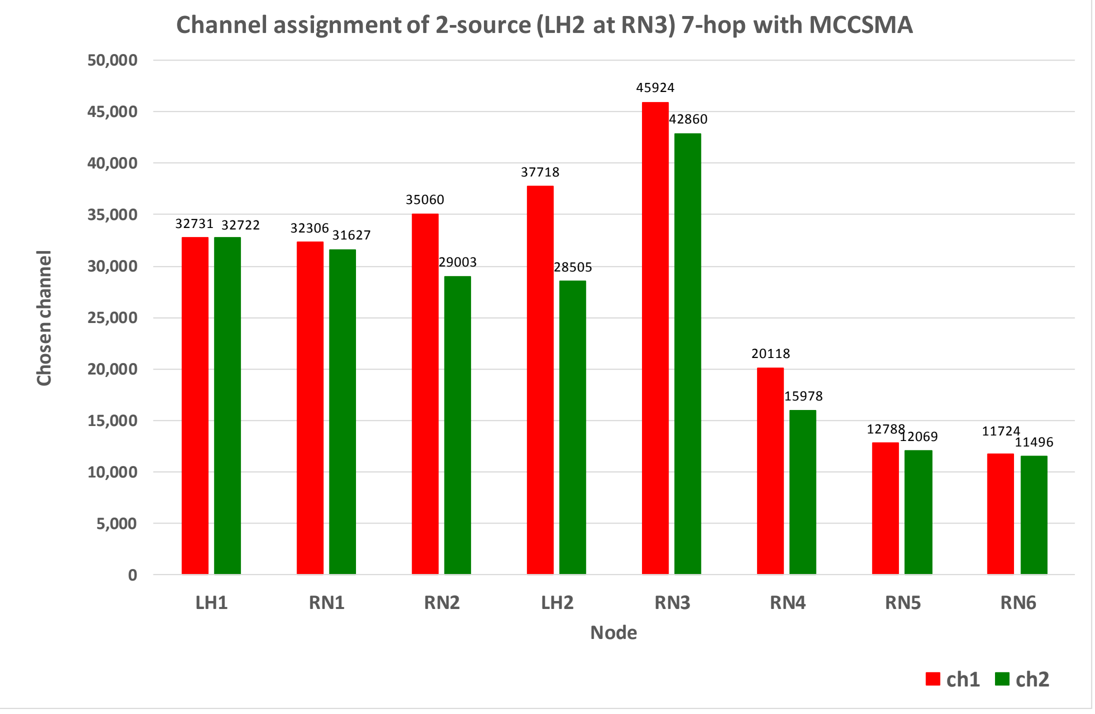

Figure 3-26 The channel assignment of MC CSMA in 2-source 7-hop network with LH2 connected at RN3

Meanwhile, the channel selection of 2HCR for 2-source 7-hop network with LH2 connected to RN3, is shown in Figure 3-27. Unlike in MC CSMA, the preference channel of 2HCR is distributed to ch1 and ch2. As the preferred channel always change after 2 hops, the collision affected by hidden node can be reduced.

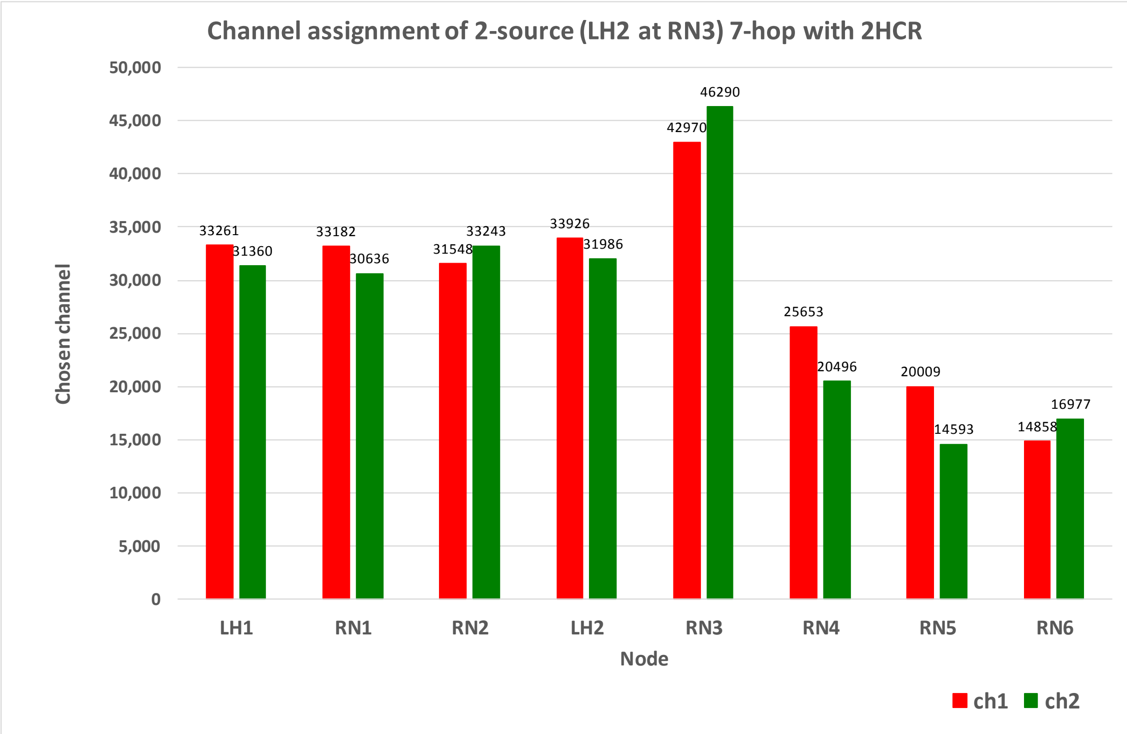

Figure 3-27 The channel assignment of 2HCR in 2-source 7-hop network with LH2 connected at RN3

Moreover, to derive a factor that provides a significant gain of 2HCR over MC CSMA in in this topology, a further observation is provided by comparing the configuration of preferred channel used in 2HCR and MC CSMA as shown in Figure 3-28. Figure 3-28 (a) denotes how all nodes in the network use ch1 as the preference, and certainly the collision occurs in all nodes from RN1 to RN6. Among them, the collision in RN3 is higher than the others as it is surrounded by three nodes (RN2, LH2, and RN4).

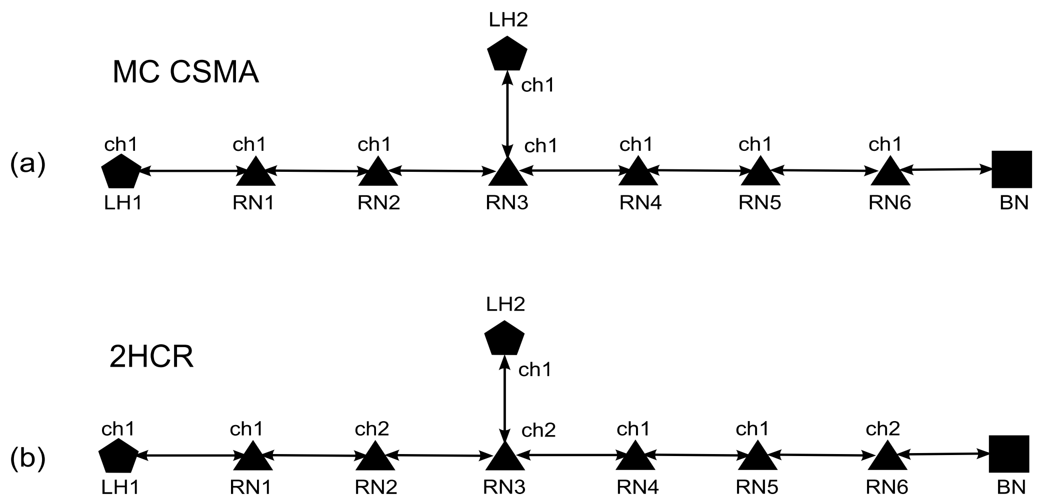

Figure 3-28 The channel assignment configuration in 2-source 7-hop network with LH2 connected at RN3 for (a) MC CSMA and (b) 2HCR

On the other hand, the channel selection of 2HCR is shown in Figure 3-28 (b). Because the nodes 2 hop away prefers to choose the distinct channel, the collision can be reduced. Therefore, the throughput of 2HCR can be higher than MC CSMA. More improvement by 2HCR compared to MC CSMA is shown on the branch of RN2, LH2, RN3, and RN4. In 2HCR, collision happens only between LH2 and RN4, whereas in MC CSMA, the collision occurs between RN2 and LH2, RN2 and RN4, also LH2 and RN4. The only one third collision possibility of 2HCR compared to MC CSMA could make the performance of 2HCR significantly better than MC CSMA.

3.6 SUMMARY

In order to provide an early warning WSN that is implemented in wide rural area, a proposed three tier WSN architecture is described in Section 3.2. As the network is configured by multihop networks in the form of chain and tree topologies, the hidden and exposed node problems can occur. As such, a multichannel MAC, namely 2HCR, is proposed to reduce the effect of hidden and exposed node problems.

By using only 2 channels, 2HCR can reduce the effect of hidden and exposed nodes as explained in Section 3.3. The algorithm of 2HCR for 2 channel utilization is addressed in Section 3.4. By using the simulation setup that is detailed in Sections 3.5, several simulations for various topologies are undertaken with the result is discussed in Section 3.6. During the simulation, the performance of 2HCR protocol is compared with the performance of 802.11b and MC CSMA protocols. The brief of the results proves that 2HCR outperforms 802.11b and MC CSMA for all topologies.

CHAPTER 4

A HYBRID MODEL FOR NETWORK THROUGHPUT ESTIMATION

4.1 INTRODUCTION

In WSN architecture described in Sections 1.1, most of networks in the system will be in the form of chain topology with branches at some points. In tier 2, a local head (LH) and a backbone node (BN) are connected by several relay nodes (RNs) as illustrated in Figure 4-1(a). LH works as a packet source, whereas BN is the last destination. If another LH is located in between LH and BN, it will be connected straight to the closest RN, or through a number of RNs depending on its distance to the closest RN. This additional link configures the branch on the existing chain as depicted in Figure 4-1 (b).

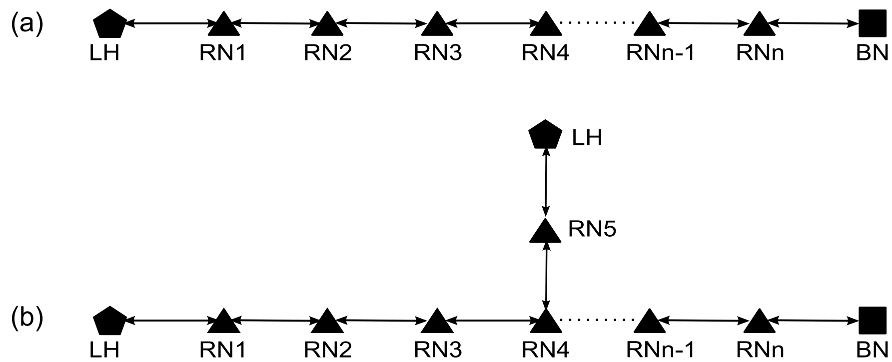

Figure 4-1 The chain network between LH and BN (a) without branch (b) with branch

Considering the hundreds square kilometres area described in Section 3.2, the networks configured by LHs, RNs, and BN can be various with many possible configurations depending on LHs locations. Therefore, it is very difficult to obtain the throughput for all these possible networks. Conducting simulation for each topology will also be very time consuming. Obtaining the throughput of the network will be more challenging if the different sources may have different data rates, as shown in Figure 4-2.

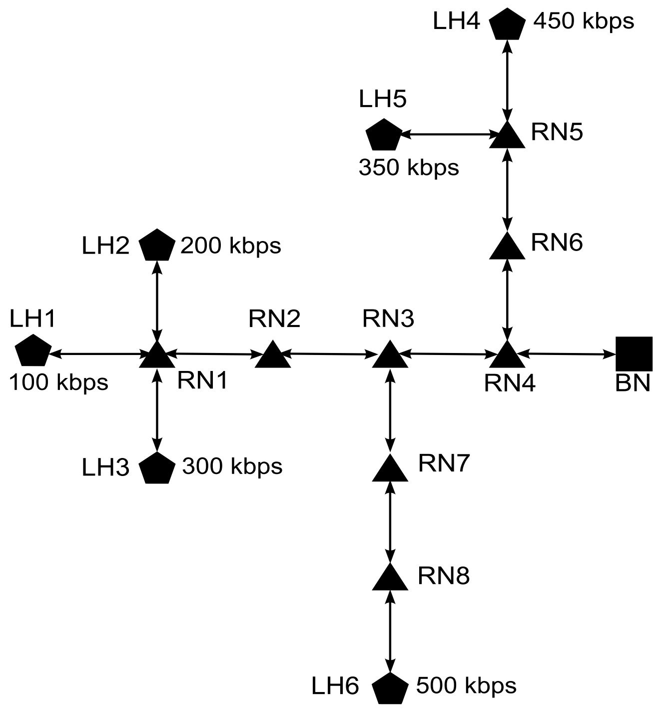

Figure 4-2 Sources with various data rates in a configuration

In order to solve this problem, a new hybrid method to estimate the throughput of complex networks is proposed in this chapter. The hybrid method combines the simulation and topology decomposition to estimate the network throughput. The procedure first chooses some basic network topologies and conducts simulation to obtain their throughput performance. Then, for a given complex network topology, the network decomposition is used to simplify it to a series of subnetworks, with each has one of the basic topologies. The throughput of each subnetwork is estimated by using the simulation results. Subsequently, the final network throughput can be estimated. The method applied in Section 4.2 and 4.3 is to estimate the throughput of networks using 2HCR protocol. In section 4.4, the estimation method is applied to MC CSMA network. Also, the method is applied to single channel network employing 802.11b MAC protocol in section 4.5. Comparison with simulation results shows that the estimation method can accurately estimate the throughput for all these MAC protocols.

4.2 ESTIMATION PROCEDURE

4.2.1 Basic Topologies

The first basic topology is 1-source chain topologies with various lengths. The configuration of 1-source topologies with hop number from 1-hop to 7-hop, are depicted in Figure 4-3.

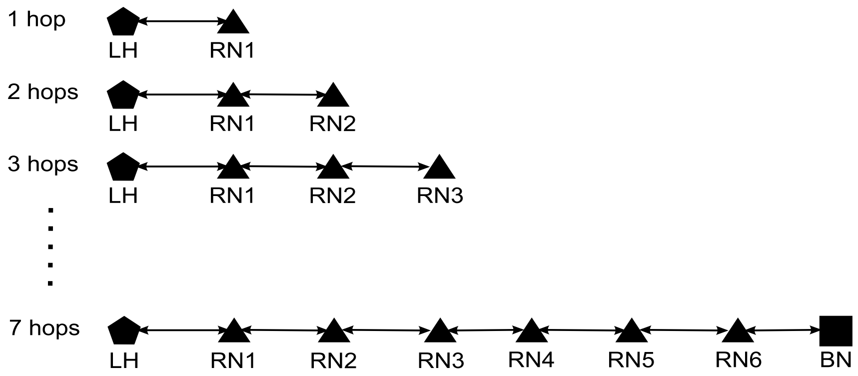

Figure 4-3 Basic topologies with 1-source

Meanwhile, the 2-source and 3-source topologies are also chosen as the basic topologies. As well as 1-source topologies, the 2-source and 3-source basic topologies consist of 1-hop to 7-hop configurations. The configuration of 2-source and 3-source topologies are depicted in Figure 4-4 and 4-5 respectively.

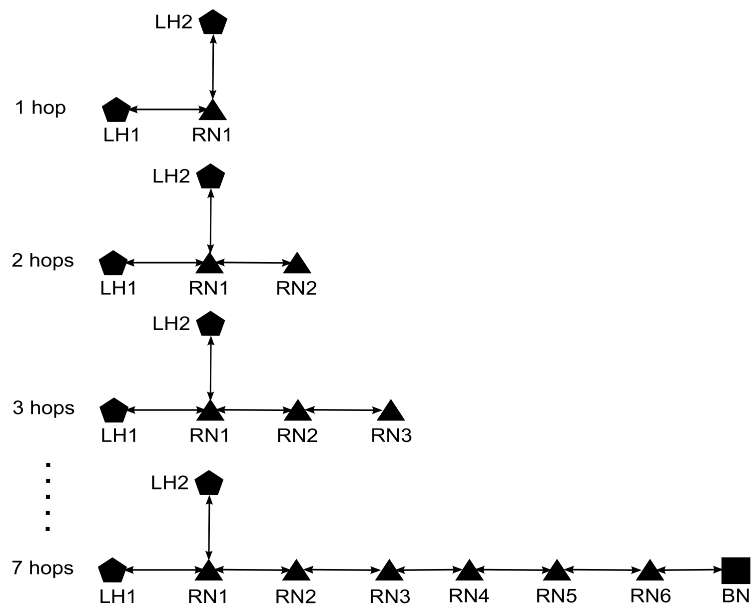

Figure 4-4 Basic network topologies with 2-source

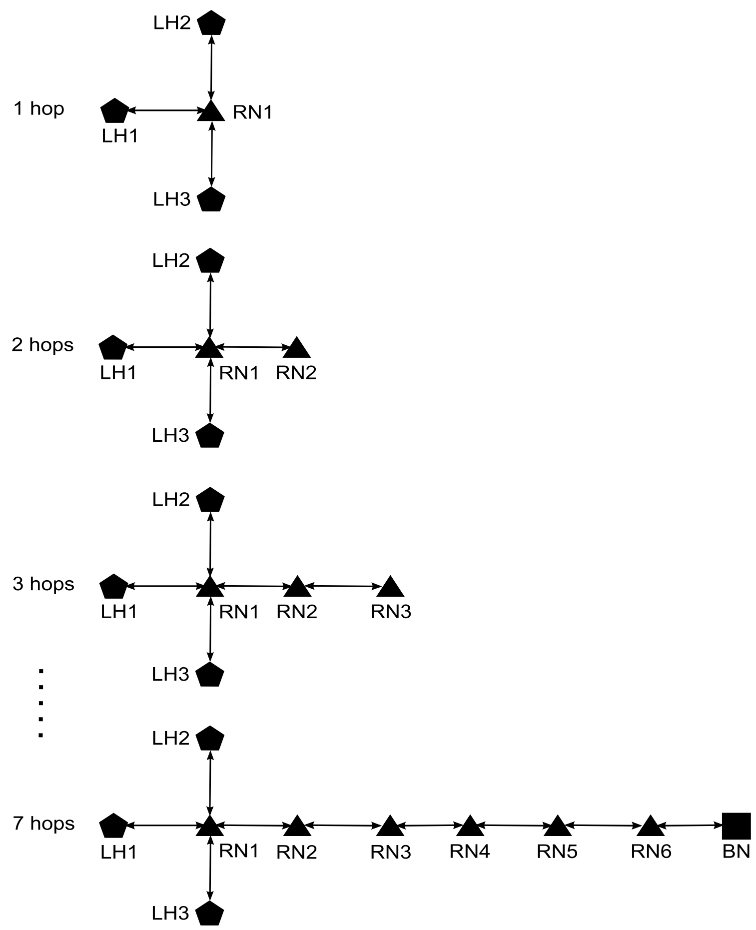

Figure 4-5 Basic network topologies with 3-source

4.2.2 Basic Topologies Simulation

Once the basic topologies have been chosen, a simulation is conducted to obtain the throughput of every topology. The throughput of 1-source topology with the chain length from 1-hop to 7 is shown in Figure 4-6. Figure 4-7 and Figure 4-8 show the throughput for 2-source and 3-source topologies respectively. For 1-hop topology, it can be seen that the throughput is the same with the input for data rate up to 700 kbps. However, the throughput remains constant at 770 kbps for the input data rate beyond 800 kbps. It denotes that the throughput has reached the maximum capacity of 1-hop network.

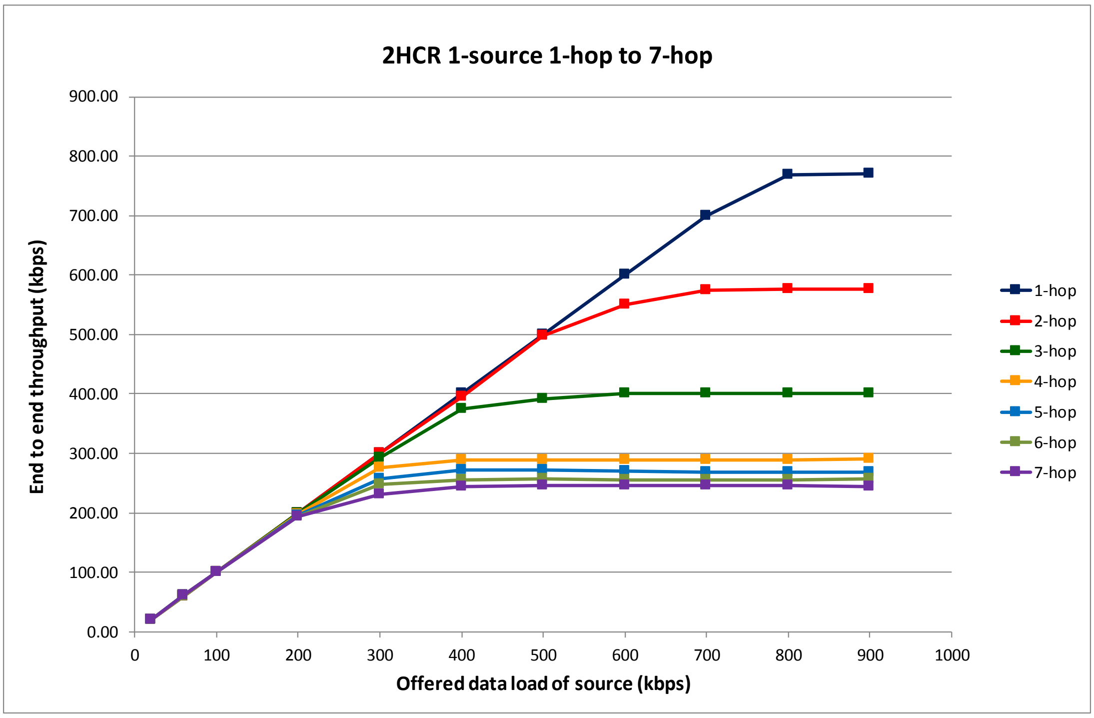

Figure 4-6 The end to end throughput of 1-source multihop networks with 2HCR protocol

Furthermore, when the hop number increases, the maximum achievable throughput reduces significantly. The throughput of 2-hop topology, for example, is 575 kbps which is 195 kbps lower than the throughput of 1-hop topology. However, such high degradation only occurs up to 4-hop topology, where its maximum throughput is 289 kbps, which is 112 kbps lower than the maximum throughput of 3-hop topology, ie., 401 kbps. For hop number beyond 4-topology, the maximum throughput decreases slightly. It is shown on the throughput of 5-hop, 6-hop, and 7-hop which is 267 kbps, 256 kbps, and 243 kbps respectively. The throughput difference between hops is less than 25 kbps. The explanation of high degradation below 3-hop, and low degradation beyond 4-hop can be referred to the discussion in Section 2.3

For 2-source multihop network, the throughput of network with 1-hop to 7-hop is illustrated in Figure 4-7. Since the number of source is two, the maximum achievable throughput is two times of the offered data on each source. The throughput of the all topology for the input data rate 20 kbps, for instance, is 40 kbps which is two times of the input data rate. However, with the increase of input data rate, the throughput becomes lower than 2 times of input data rate. In 1-hop topology, for instance, the input data rate of 300 kbps achieves only 591 kbps rather than 600 kbps. Afterwards, the throughput stays constant at 769 kbps as the maximum achievable throughput.

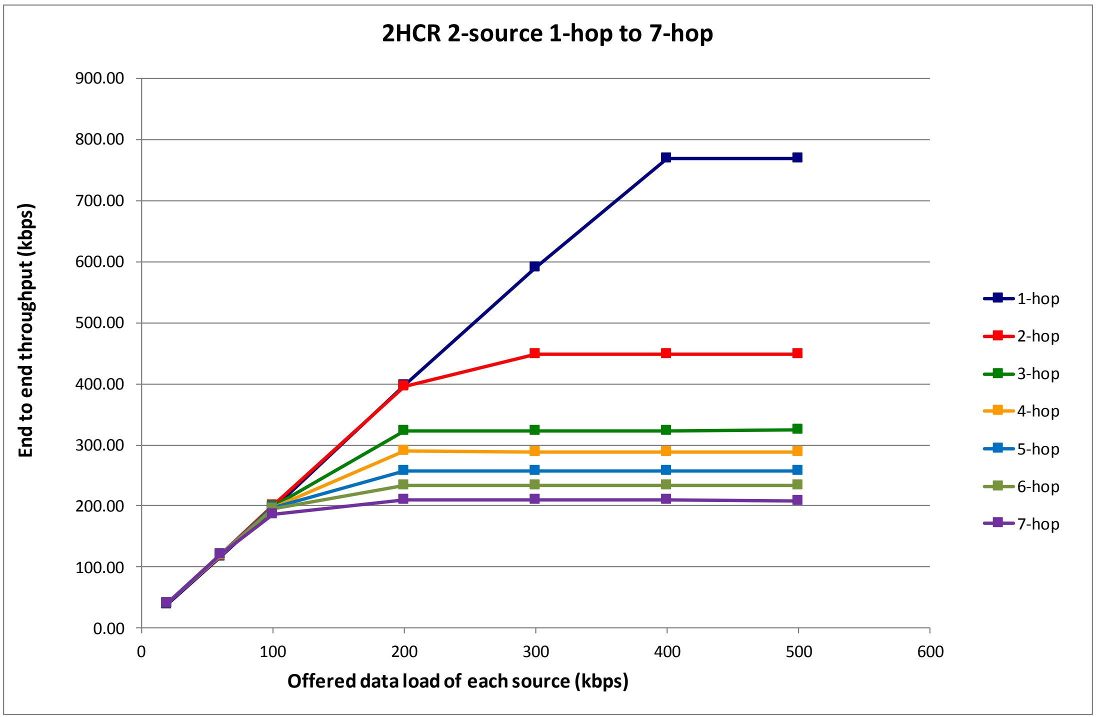

Figure 4-7 The end to end throughput of 2-source multihop networks with 2HCR protocol

If the hop number is increased to 2-hop, the maximum throughput declines significantly as occurring in 1-source network case. For this 2-hop topology, the maximum achievable throughput is 448 kbps, which is 321 kbps lower than the maximum throughput of 1-hop network. The high throughput degradation still happens for 3-hop topology with the maximum throughput of 323 kbps that is 125 kbps lower than the throughput of 2-hop topology. However, beyond this hop number, the degradation is lower. With maximum throughput of 288 kbps, 257 kbps, 233 kbps, and 209 kbps for 4-hop, 5-hop, 6-hop, and 7-hop topologies respectively, the throughput degradation is less than 40 kbps. In addition, in comparison with 1-source topologies, the maximum throughput of this 2-source topologies is lower as the multisource collision is happening apart of the collision caused by the chain structure.

The throughput of 3-source topologies is shown in Figure 4-8. With the input data rate of 20 kbps for each source, the throughput is 60 kbps for all of hop numbers. It indicates the aggregation of 3 sources input data rates. The similar aggregation result is achieved for the input data rate of 60 kbps, although for several topologies, the throughput is less than 180 kbps. Moreover, when the input data rate is increased, the throughput of each topology obtains the distinct result, and achieves various maximum throughputs. As it happens in 1-source and 2-source cases, the maximum throughput is reduced along with the increase of the hop number. The maximum throughput of 1-hop to 7-hop topology is 768 kbps, 448 kbps, 323 kbps, 286 kbps, 256 kbps, 231 kbps, and 210 kbps respectively. It can be seen that the throughput degradation is high until 3-hop topology, with the degradation from 1-hop to 2-hop and 2-hop to 3-hop is 320 kbps and 125 kbps respectively. However, the degradation from 3-hop to 4-hop until 6-hop to 7-hop is less than 40 kbps. Comparing with 2-source case, the maximum throughput of 3-source is similar for the same hop number. The additional source for 3-source topology has not much impact to the overall throughput.

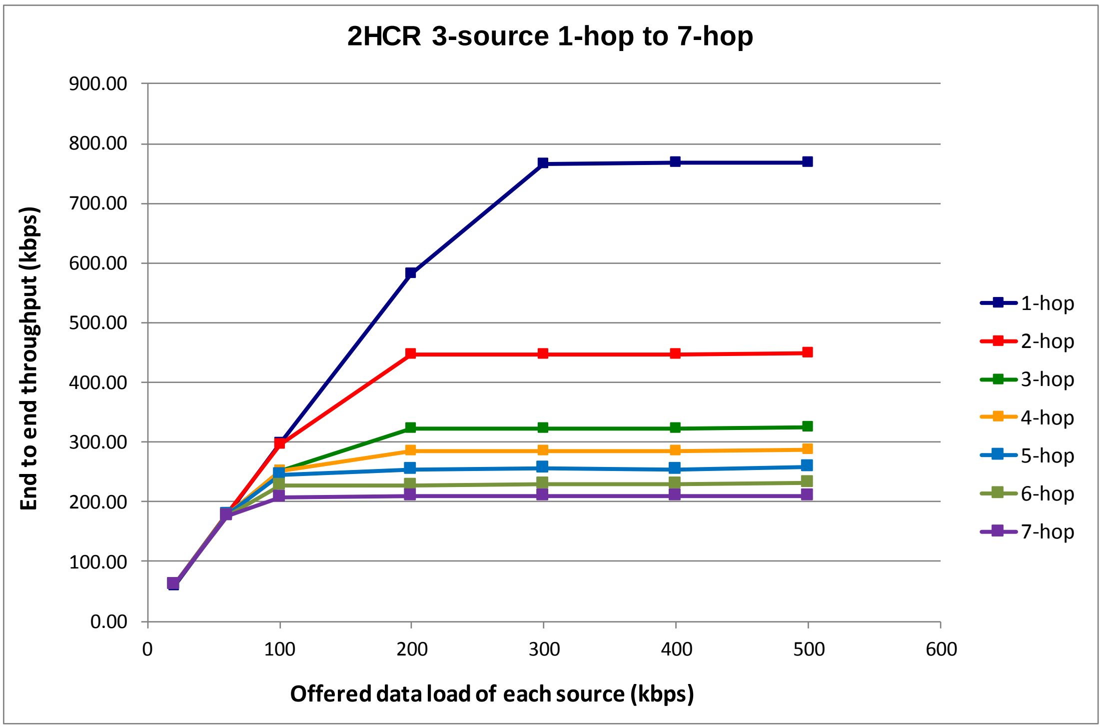

Figure 4-8 The end to end throughput of 3-source multihop networks with 2HCR protocol

The results in Figure 4-6, 4-7, and 4-8 are obtained from the simulation of 2HCR protocol without employing RTS/CTS hand shake. The simulation of 2HCR with RTS/CTS handshake is also provided as follows. The end to end throughput of 1-source multihop network with 2HCR protocol with RTS/CTS is shown in Figure 4-9. It shows that the large degradation occurs from 1-hop to 4-hop topologies. With the maximum achievable throughput of 587 kbps, 486, kbps, 332 kbps, and 199 kbps, for 1-hop, 2-hop, 3-hop, and 4-hop respectively, the throughput degradation is more than 100 kbps when hop count is increased by one. On the other hand, from 4-hop to 7-hop topologies, the degradation is smaller with only less than 25 kbps. In this case, the maximum throughput of 5-hop is 178 kbps, 6-hop is 158 kbps, and 7-hop is 143 kbps. Moreover, in comparison with the simulation result of 2HCR protocol without RTS/CTS, as shown in Figure 4-6, the throughputs of all topologies with RTS/CTS are lower. As explained in Section 3.6.3, the additional RTS and CTS packets can reduce the throughput as they increase the traffic, and cause more contention with the data packets, particularly when source data rate is already high.

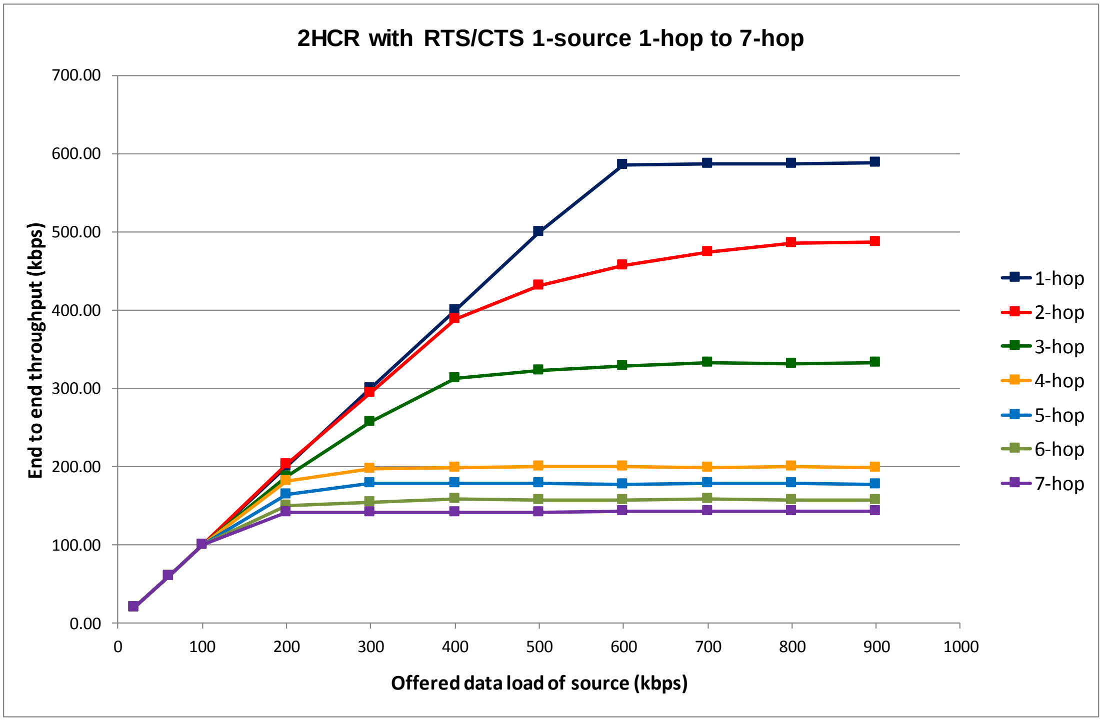

Figure 4-9 The end to end throughput of 1-source multihop networks with 2HCR protocol enabling RTS/CTS

Furthermore, the simulation result of 2-source multihop network with 2HCR protocol enabling RTS/CTS is shown in Figure 4-10. The maximum end to end throughput of each topology from 1-hop to 7-hop topologies is 607 kbps, 378 kbps, 253 kbps, 190 kbps, 162 kbps, 142 kbps, and 126 kbps respectively. Again, it is shown that the throughput degradation from 1-hop to 4-hop topologies is high with the difference between end to end throughput is more than 60 kbps. However, the throughput degradation from 4-hop to 7-hop is lower with the difference between maximum throughput is less than 30 kbps. Meanwhile, by comparing these results with the throughputs of 1-source topologies, the throughputs of all topologies in 2-source cases are lower, excepted in 1-hop topology. It may due to the statistical multisource gain that results more packets can be received by the last destination than in 1-source, even though the collision of packets delivered by the different sources also occurs. In addition, in comparison with the simulation result of 2HCR topology without RTS/CTS, the throughput of the same topology is smaller.

Figure 4-10 The end to end throughput of 2-source multihop networks with 2HCR protocol enabling RTS/CTS

Finally, the end to end throughput of 3-source multihop network with 2HCR protocols activating RTS/CTS is denoted in Figure 4-11. Similar with the results in 1-source and 2-source networks, the high throughput degradation in 3-source network also happens between 1-hop and 4-hop topologies. With the throughput of 607 kbps, 372 kbps, 231 kbps, and 180 kbps for 1-hop, 2-hop, 3-hop, and 4-hop topologies respectively, the throughput degradation associated with the increase of the hop number is more than 50 kbps. The highest throughput degradation, which is 235 kbps, is yielded when the hop number is increased from 1-hop to 2-hop. On the other hand, the throughput degradation slightly decreases when the hop number is increased from 4-hop into 5-hop, 6-hop, and 7-hop. For 5-hop, 6-hop, and 7-hop with the maximum throughput of 153 kbps, 140 kbps, and 125 kbps respectively, the degradation is under 30 kbps. Moreover, compared with the throughput of 2-source scheme, the throughput of 3-source scheme for the same hop number is lower, excepted in 1-hop topology.

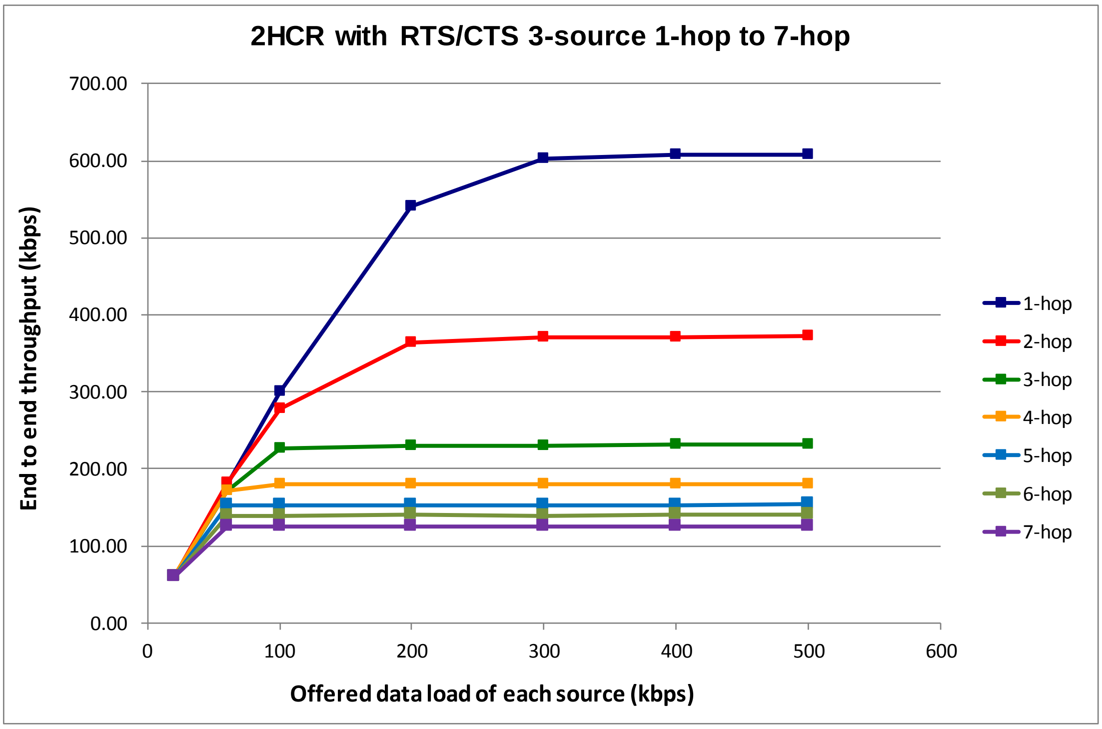

Figure 4-11 The end to end throughput of 3-source multihop networks with 2HCR protocol enabling RTS/CTS

4.2.3 Decomposition of the Complex Network

In the estimation procedure, decomposition is undertaken by separating the complex network into subnetworks available in basic topologies. Then it is followed by simplifying the network iteratively for the entire complex network, until the iterative result gives the last topology that matches with one of basic topologies. Furthermore, when defining a subnetwork, the end of the subnetwork is the last node before the next branch. For the network in Figure 4-2, the entire network is decomposed into subnetworks as shown in Figure 4-12 (a).

At the first stage of decomposition, the entire network has subnetworks: transformed node (TFN) 1, TFN2, and TFN3. Subnetwork TFN1 is configured by LH1, LH2, LH3, and RN2 which is the same as the basic 3-source 2-hop topology. On the other hand, TFN2 consists of LH6, RN7, and RN8 which configure 1-source 2-hop network. Meanwhile, TFN3 consists of LH4, LH5, RN5, and RN6 which is in the form of 2-source 2-hop topology. With the representation of TFNs, the entire network now can be illustrated as a network in Figure 4-12 (b). As this decomposed topology has not matched with any of basic topologies, it is simplified into the last topology depicted in Figure 4-12 (c). To obtain a topology that available in basic topologies, TFN1, TFN2 and RN3 are transformed into TFN 4 to finally perform 2-source 1-hop network.

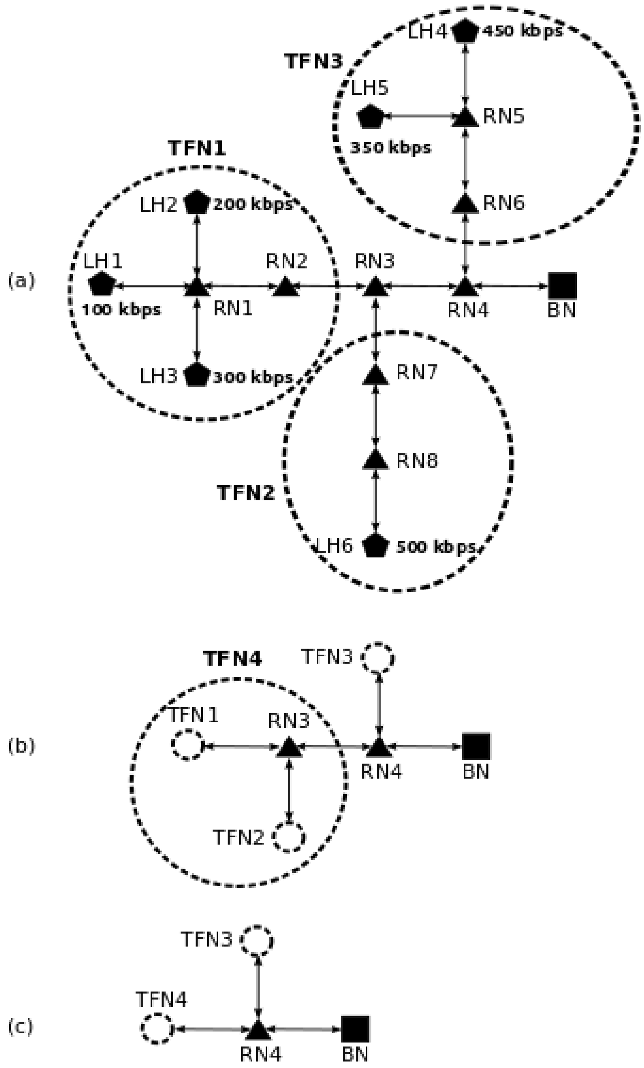

Figure 4-12 Decomposition of complex network

In order to obtain the throughput estimation of the complex network, an iterative calculation process is undertaken until finding the throughput of the last topology. For Figure 4-2, the calculation process is provided by following steps. In the network transformation from Figure 4-12 (a) into Figure 4-12 (b), the throughput of TFN1, TFN2, and TFN 3 must be yielded. Such throughputs will be used as the input data rate for network in Figure 4-12 (b). The throughput of each TFN refers to the throughput of the basic topology that has the same configuration.

The throughput of TFN1, for instance, is the throughput of basic 3-source 2-hop topology. Thus, it can be obtained from 2-hop curve available in Figure 4-8. However, the curves in such figure are obtained from an assumption that all sources have the same data rate. In contrast, the input data rate of each source in TFN1 is different. To solve this mismatching, the input data rate of TFN1 is yielded from the average value of the three sources. As such, the input data rate is 200 kbps which is the average of 100, 200, and 300 kbps. The same way employed to obtain the throughput of TFN2 and TFN3, is also used to simplify the topology in Figure 4-12 (b) into 4-12 (c). Finally, the throughput of the last topology must refer to the throughput of 2-source 2-hop network. This last throughput is defined as the throughput estimation of the entire network in Figure 4-12 (a). This mechanism could be represented by pseudocode shown in Figure 4-13.

```
Find all of the network edges;
Distinguish LH from BN by its identity;

//Recognizing the chain
Point to an LH;
if ( there is a branch located one hop after LH) {
    Find number of LH connected to this branch;
    Calculate the average data rate of all LHs in the branch;
    Find the next branch;
    The end of the chain is the last node before the branch;
    Find the chain hop number;   //between LH to the last node
    Use number of LH and hop as the chain configuration information;
    Compare the configuration with the basic configuration;
    Find the throughput of the chain by using average data rate as the input;
    Assign the chain as a TFN;
    }
Repeat the above process with TFN as the edge of the chain;
Repeat the process until finding BN as the last node;
```

Figure 4-13 Pseudocode of decomposition procedure

4.3 EVALUATION OF THE ESTIMATION MODELS FOR COMPLEX NETWORKS WITH 2HCR

To evaluate the estimation models, the prediction is undertaken for the complex networks denoted in Figure 3-9 and 3-10 in Section 3.5. Albeit they are not too complex to be estimated, they already have the simulation result provided in Section 3.6. This simulation result will be compared with the prediction result to evaluate the accuracy of the estimation model.

The first examination is undertaken for 2-source 4-hop networks with shifted LH2 location as illustrated in Figure 3-9 (a) (b). The comparison between the prediction and the simulation is shown in Figure 4-14. The green curves in Figure 4-14 represent the throughput of the topology in Figure 3-9 (a) where LH2 is connected to RN2, whilst the brown curves represent the throughput of the topology in Figure 3-9 (b) where LH2 is connected to RN3. As it is shown in the Figure 4-14, with the estimated maximum throughput of 323 kbps and the simulated maximum throughput of 332 kbps, the maximum deviation between the prediction and the simulation for the first scenario is 2.71 %. Meanwhile, for the second scenario, the estimated and simulated throughput is 448 kbps and 482 kbps respectively. Thus, the maximum deviation for this scenario achieves 7.05 %. Generally, the estimation result can be considered quite accurate if the deviation is less than 10 % limit. With this consideration, both estimation results can be categorized as accurate.

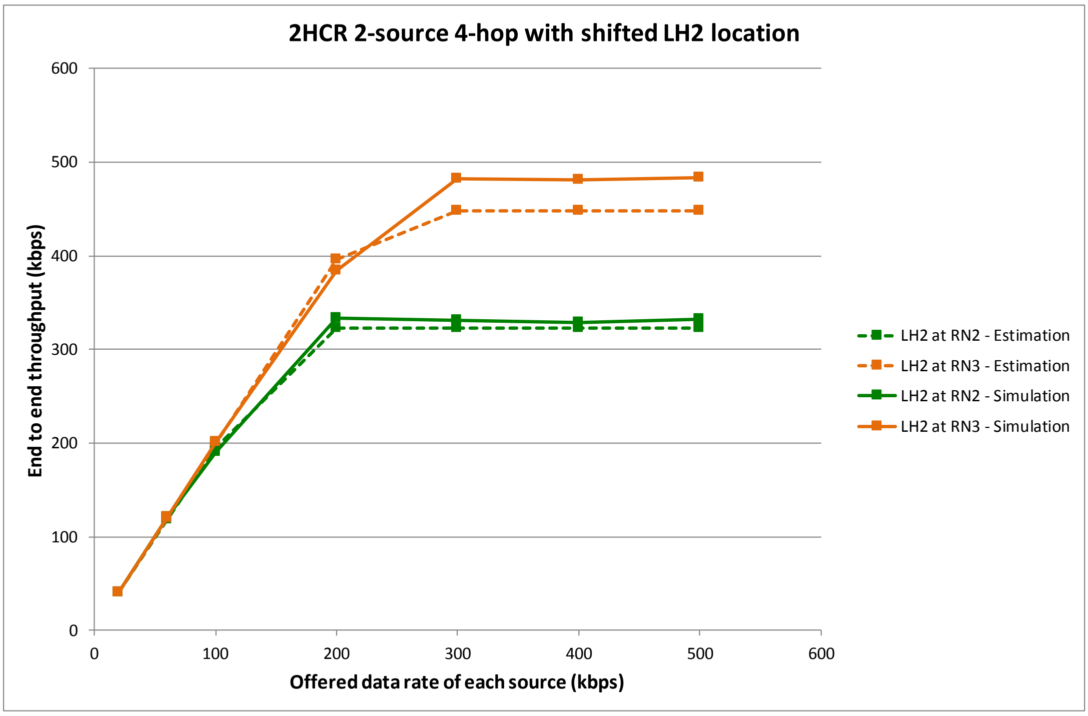

Figure 4-14 Comparison between estimation and simulation for 2-source 4-hop shifted LH2 location with 2HCR protocol

Meanwhile, the examination is also provided for the 3-source 4-hop topologies with shifted LH3 location as illustrated in Figure 3-9 (c) (d). The comparison between the estimation and simulation results is depicted in Figure 4-15. For LH3 connected to RN2, the predicted maximum throughput of 323 kbps and the simulated throughput of 300 kbps give the maximum deviation of 7.12 %. Meanwhile, for LH3 connected to RN3, the maximum deviation reaches 9.68 % as the predicted and the simulated throughput in this scenario is 448 kbps and 496 kbps respectively. Both deviations are higher than in 2-source 4-hop network, however the deviation is still under 10%.

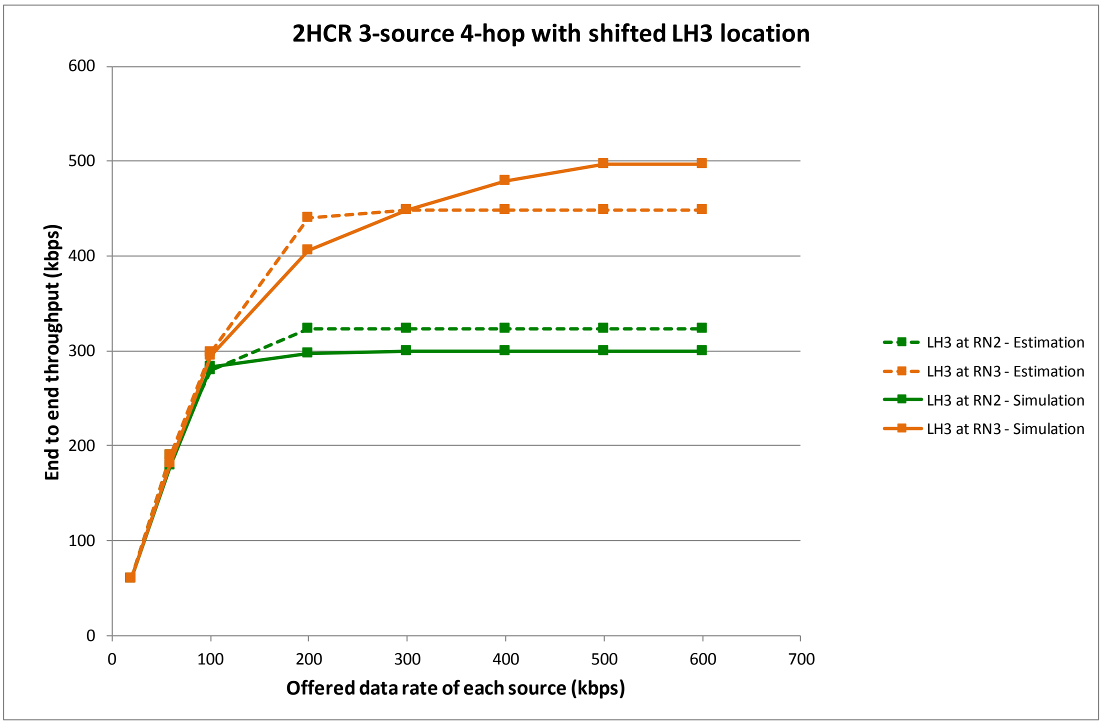

Figure 4-15 Comparison between estimation and simulation for 3-source 4-hop shifted LH3 location with 2HCR protocol

If the chain is extended into 7-hop, the comparison between the estimation and the simulation for 2-source topologies with shifted LH2 location is illustrated in Figure 4-16. For the first scenario where LH2 is connected to RN2, the estimation throughput is 233 kbps while the simulation throughput is 247 kbps, and therefore the maximum deviation is 5.67 %. On the other hand, for the second scenario where LH2 is connected to RN3, the estimation throughput is 257 kbps whilst the simulation throughput is 286 kbps. Thus, the maximum deviation reaches 10.14 %. While the deviation of the first scenario is less than 10 %, the deviation of the second scenario is more than 10 %. In addition, compared with the result in 2-source 4-hop, the maximum deviation of 2-source 7-hop topology is higher.

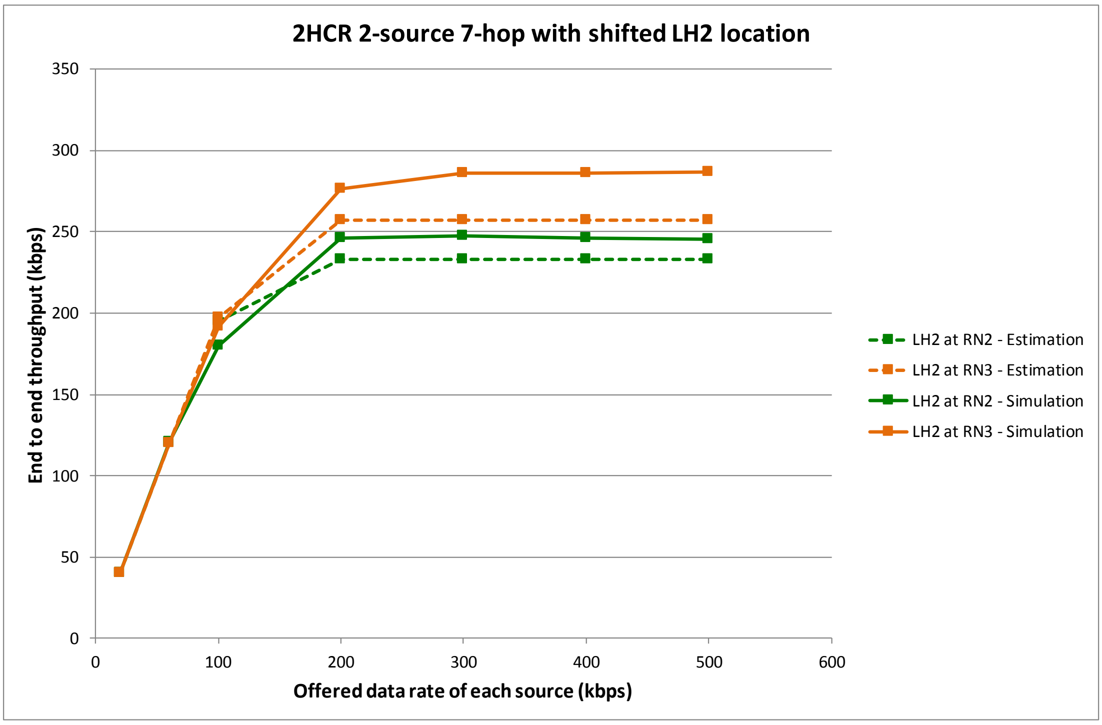

Figure 4-16 Comparison between estimation and simulation for 2-source 7-hop shifted LH2 location with 2HCR protocol

Furthermore, the comparison of the prediction result with the simulation result for 3-source 7-hop topologies with shifted LH3 location is depicted in Figure 4-17. For LH3 connected to RN2, the maximum deviation achieves 8.27 %. This is obtained through the predicted maximum throughput of 233 kbps and the simulated throughput of 254 kbps. On the other hand, if LH3 is connected to RN3, the maximum deviation reaches 7.55 % for the predicted throughput of 257 kbps and the simulated throughput of 278 kbps. For these results, the estimation model for this topology is categorized accurate. However, in comparison with the previous results, the deviations in this topology gives a different trend, where the deviation of the first scenario is higher than the deviation of the second scenario, whereas in the other topologies, the deviation of the first scenario is always lower than the deviation of the second scenario.

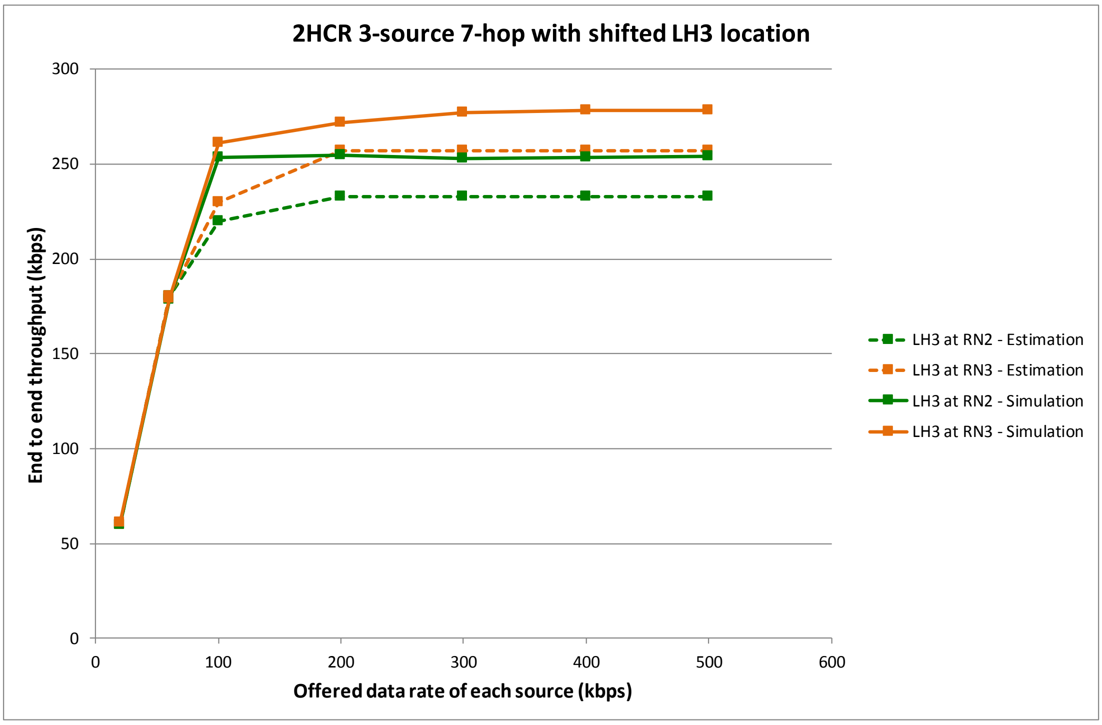

Figure 4-17 Comparison between estimation and simulation for 3-source 7-hop shifted LH3 location with 2HCR protocol

The evaluation of the prediction results is also undertaken for all topologies with 2HCR protocol enabling RTS/CTS handshake. Figure 4-18 illustrates the comparison between the prediction and the simulation throughput for 2-source 4-hop network with shifted LH2 location, and with 2HCR protocol activating RTS/CTS. For LH2 connected to RN2, the predicted throughput of 253 kbps and the simulation throughput of 262 kbps obtain the deviation of 3.44 %. On the other hand, for LH2 connected with RN3, the predicted throughput of 377 kbps and the simulation throughput of 443 kbps obtain the deviation of 14.90 %. As such, the deviation of the first scenario is lower than 10 %, while the deviation of the second scenario is higher than 10 %. To investigate the cause of such high deviation, a further observation will be provided in the last paragraphs of this Section.

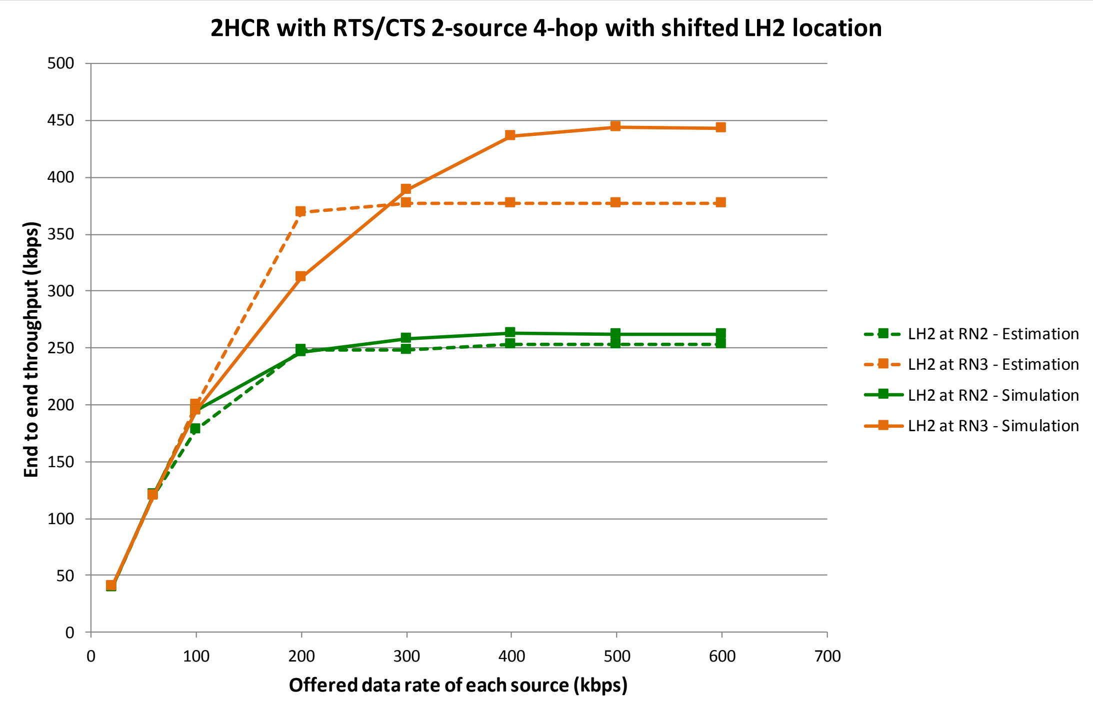

Figure 4-18 Comparison between estimation and simulation for 2-source 4-hop shifted LH2 location with 2HCR RTS/CTS protocol

Furthermore, the estimated and the simulated throughput of 3-source 4-hop network with shifted LH3 location is depicted in Figure 4-19. For the first scenario where LH3 is located near RN2, the estimation yields the maximum throughput of 253 kbps, while the simulation gives the maximum achievable throughput of 239 kbps. For these results, the deviation is then 5.53 % which is under the limit of 10 %. On the other hand, in the second scenario where LH3 is located near RN3, the estimation gives the maximum throughput of 377 kbps, which is deviated 18.75 % from the simulation result that reaches 464 kbps. As well as in previous 2-source 4-hop topology, the high deviation is also obtained in the second scenario of this 3-source 4-hop topology. The further investigation will be provided in the last paragraphs of this Section.

Moreover, for 2-source 7-hop network with shifted LH2 location, the comparison between the prediction and the simulation result is denoted in Figure 4-20. It is likely the estimation derives a result closed to the simulation result.

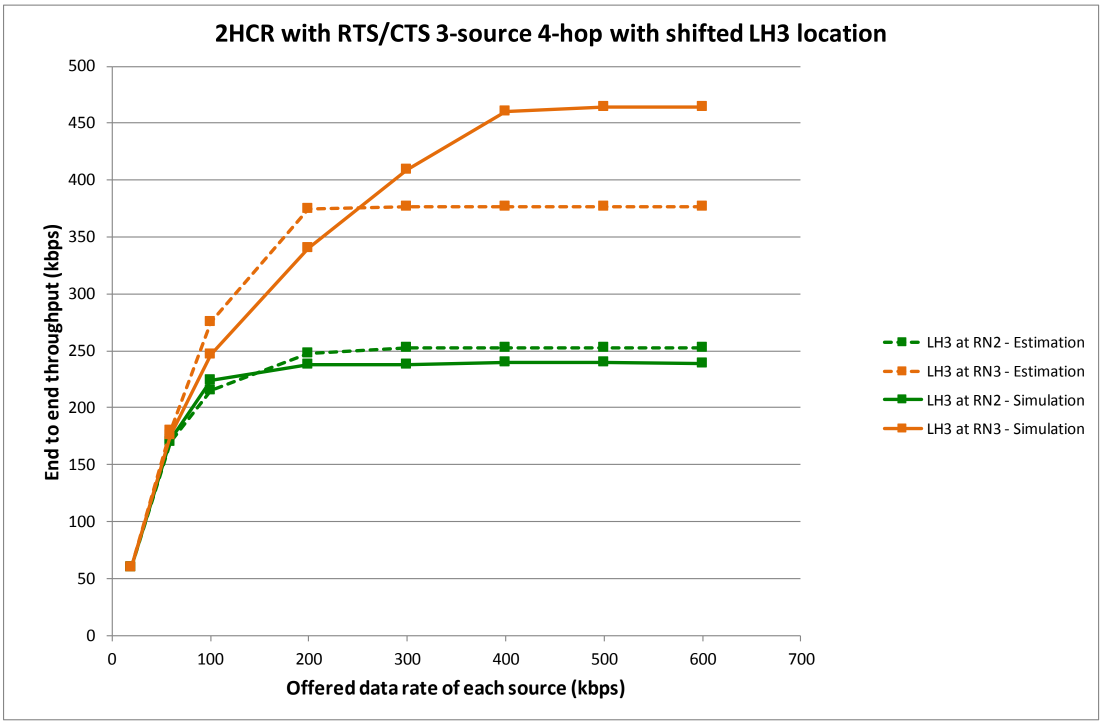

Figure 4-19 Comparison between estimation and simulation for 3-source 4-hop shifted LH3 location with 2HCR RTS/CTS protocol

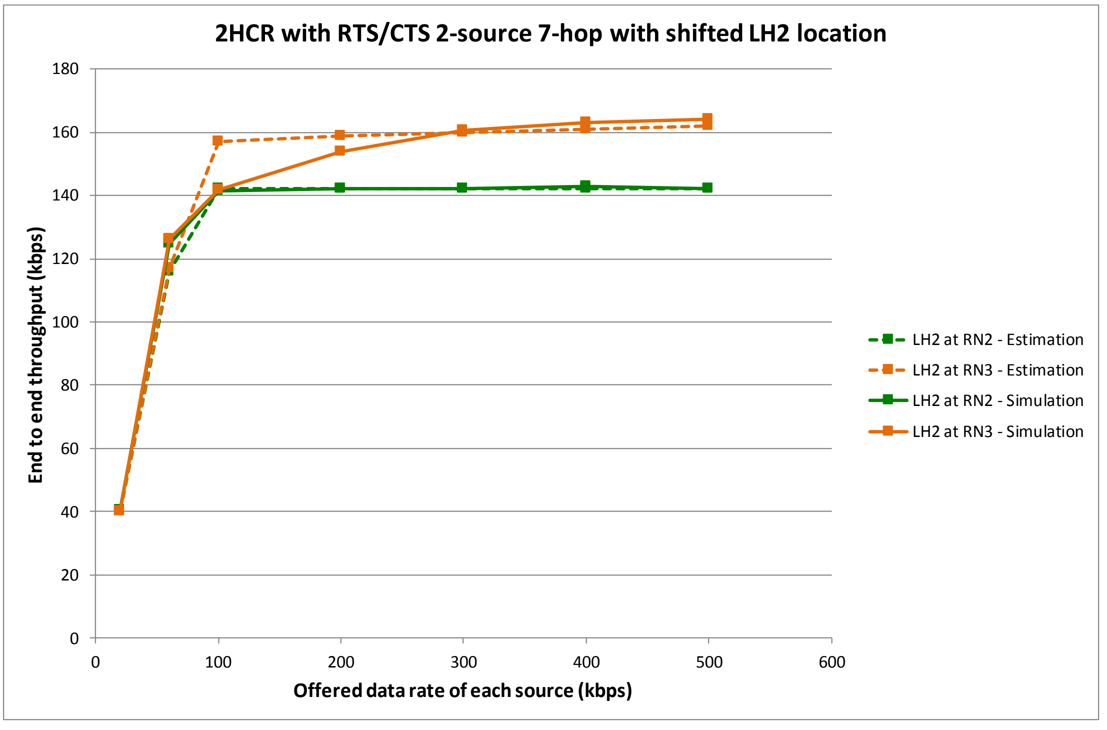

Figure 4-20 Comparison between estimation and simulation for 2-source 7-hop shifted LH2 location with 2HCR RTS/CTS protocol

In Figure 4-20, if LH3 is connected to RN2, the estimated maximum throughput derives 142 kbps as well as obtained by the simulation. Therefore, the deviation for this case is 0 %. Concurrently, if LH3 is connected to RN3, the estimated maximum throughput is 162 kbps, while the throughput from the simulation is 164 kbps. For these results, the deviation becomes 1.22 %. It can be seen that the deviations in this topology is the lowest maximum deviation among the previous results.

Finally, the throughput of the estimation and simulation results for 3-source 7-hop network with shifted LH3 location is depicted in Figure 4-21. For the first scenario where LH3 is located near RN2, the estimation and simulation give the maximum throughputs of 142 kbps and 150 kbps respectively, and therefore the deviation yields 5.33 %. On the other hand, for the second scenario where LH3 is located near RN3, the maximum throughput of the estimation is 162 kbps, while the simulation result is 173 kbps, and thus obtains 6.36 % deviation. As such, the estimation result for this topology provides less than 10 % deviation.

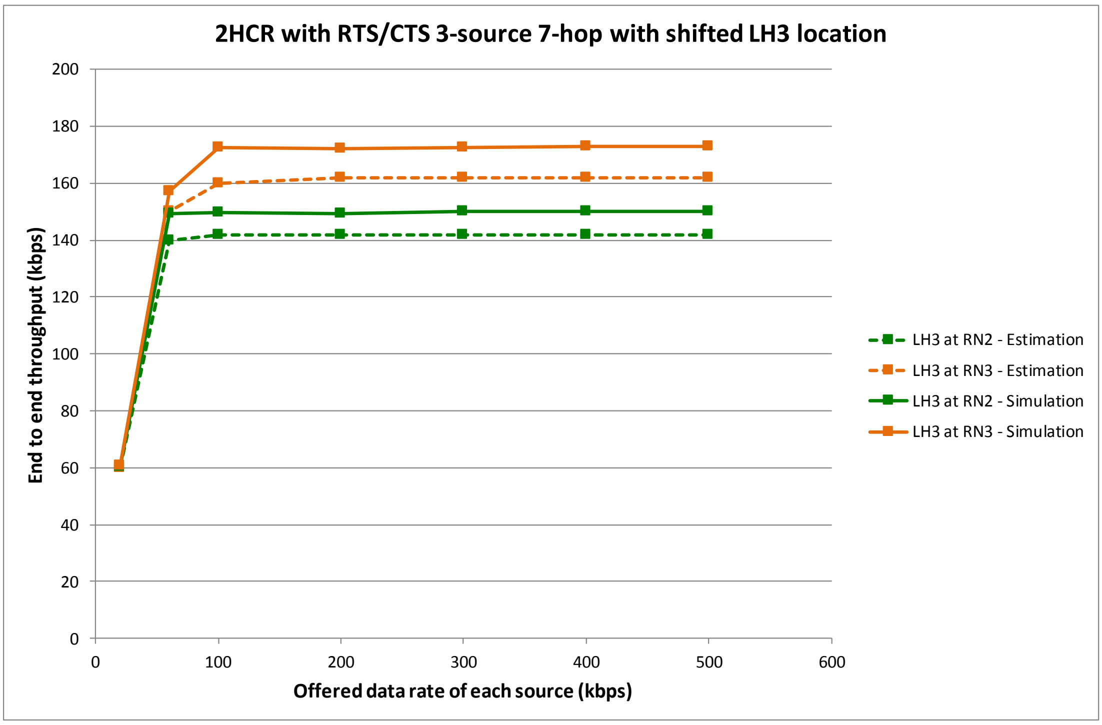

Figure 4-21 Comparison between estimation and simulation for 3-source 7-hop shifted LH3 location with 2HCR RTS/CTS protocol

To be concluded, all comparisons obtained from networks working with 2HCR protocol have shown that, in general, most estimation results reach the maximum deviation less than 10 %. There are three of sixteen estimations which derive the maximum deviation higher than 10 %. Those high deviations are yielded from the estimation of the second scenario where one of sources (LH2 or LH3) is connected to RN3. A further observation to find the cause of this high deviation is provided in the next paragraphs. In addition, the average deviation of the estimation in 2HCR protocol is 7.11 %.

The maximum deviation that reaches more than 10 % in throughput estimation with 2HCR protocol indicates unexpected behaviour in the simulation process which has not been considered in the estimation procedure. The maximum deviation reaches 18.75 % in the second scenario of 3-source 4-hop with 2HCR RTS/CTS. To find the cause of this phenomenon, a comparison between the simulation and estimation is undertaken by the following investigation.

The observation is performed by comparing the individual data rate of RN2, RN3, and BN obtained from the estimation and simulation of 3-source 4-hop network with 2HCR RTS/CTS protocol. The comparison is provided for the offered data rate of 500 kbps, where the highest deviation occurs. The individual data rate from the simulation is yielded by measuring the data rate of RN2, RN3, and BN through the simulation of entire network. On the other hand, the result from the estimation method is obtained from the following steps.

First, LH1, LH2, RN1, and RN2 are transformed into TFN1 as shown in Figure 4-22 (a). The second step is obtaining the throughput of this network. As the three nodes configure 2-source 2-hop network, the throughput then refers to the throughput of basic 2-source 2-hop network. With input data rate of 500 kbps, the throughput of TFN1 is 377 kbps.

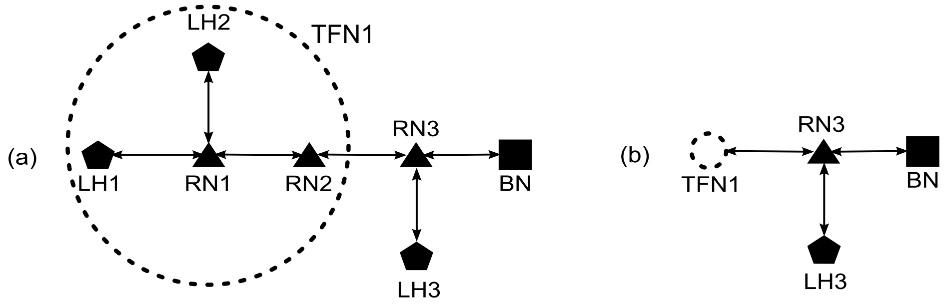

Figure 4-22 Decomposition of 3-source 4-hop network with LH3 located adjacent RN3 with (a) the original topology (b) the transformed topology

By using the result in the second step, the last step is running the simulation to obtain the individual data rate of TFN1, RN3, and BN. This data rates are compared with the data rates of RN2, RN3, BN obtained by the simulation of entire network as shown in Table 4-1.

Table 4-1 The comparison of nodes' individual data rate obtained from estimation and simulation for the offered data rate of 500 kbps

	TFN1 (for estimation) and RN2 (for simulation) (kbps)	rn31rx (kbps)	rn32rx (kbps)	bn1rx (kbps)	bn2rx (kbps)	bn tot (kbps)
Estimation	377	308	320	183	194	377
Simulation	41	40	486	36	428	464

In Table 4-1, the second column indicates the data rate of TFN1, ie. from the estimation, and RN2, ie., from the simulation of entire network. The notation rn31rx in the third column represents the data rate of packet coming from RN2 (or TFN1) to RN3. Meanwhile, rn32rx indicates the data rate of packet arriving from LH3 at RN3. On the other hand, bn1rx shows the data rate of packet at BN which is originally from RN2, while bn2rx is originally from LH3. Finally, bn tot is the total data rate of packet received by BN, ie., the network throughput.

Furthermore, in the estimation method, a small difference between data rate in RN2 and LH3 shows that the individual data rate accepted in RN3 is quite balance, as the packets coming from both RN2 and LH3 still have a strong competition. This competition still occurs until the packets reach the destination. On the other hand, in the simulation method, a low data rate at RN2 which is smaller than one tenth of data rate at LH3, gives opportunity to LH3 to dominate the network by injecting much more packet. As a result, both RN3 and BN are flooded by packets from LH3 rather than packets from RN2. This explanation has answered the behaviour of the entire network simulation which has not been considered in the estimation procedure.

4.4 EVALUATION OF THE ESTIMATION MODELS FOR COMPLEX NETWORKS WITH MC CSMA

The same procedure is also applied to MC CSMA to evaluate the prediction accuracy for another type of protocol. For this evaluation, the throughput of basic topologies needs to obtain through simulations with MC CSMA protocol. As well as with 2HCR protocol, the simulation is provided for both disabled and enabled RTS/CTS handshake. For the earlier, the throughput of 1-source multihop networks is shown in Figure 4-23.

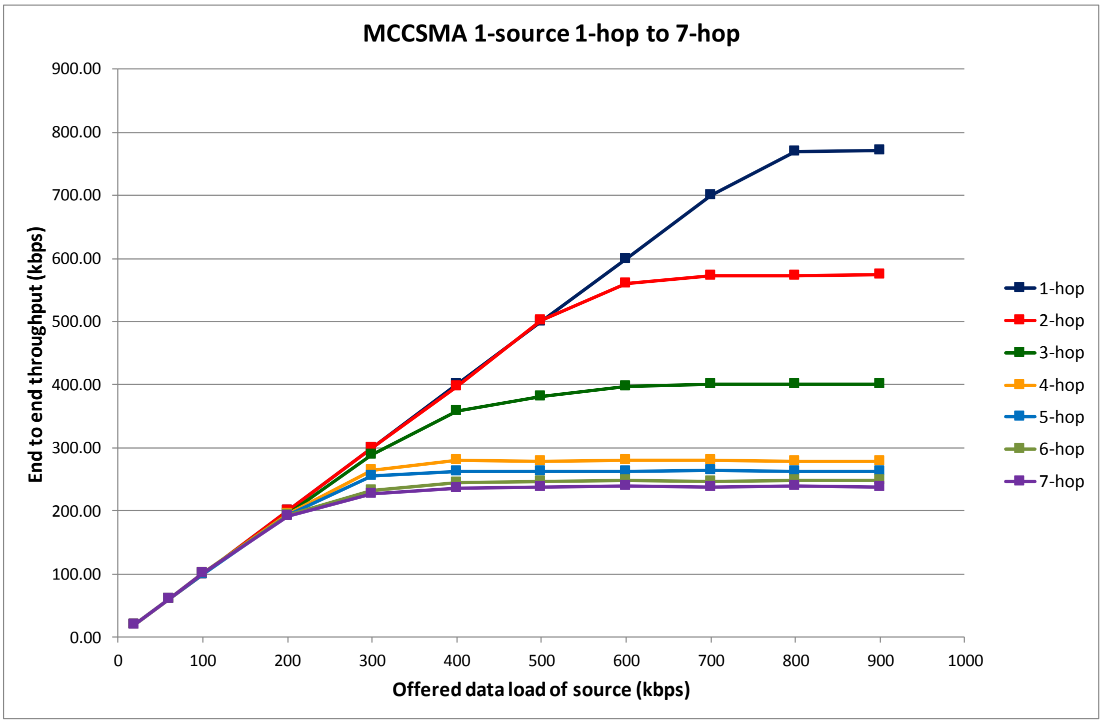

Figure 4-23 The end to end throughput of 1-source multihop networks with MC CSMA protocol

For 1-hop topology, the end to end throughput is the same as the input data rate excepted for the input data rate of 800 kbps and 900 kbps. The throughput of both input data rates is 770 kbps which may be the maximum capacity of this 1-hop topology. This maximum throughput is the same with the maximum throughput in 2HCR. Furthermore, the maximum achievable throughput reduces if the hop number is increased. The high degradation is obtained when the hop number is increased from 1-hop topology into 2-hop, 3-hop, and 4-hop. With the throughputs of 1-hop to 4-hop topologies which are 770 kbps, 574 kbps, 401 kbps, and 279 kbps respectively, it is denoted that the degradation achieves more than 120 kbps. In contrast, the throughput degradation from 4-hop to 7-hop is smaller. For the throughputs of 5-hop to 7-hop which are 263 kbps, 248 kbps, and 238 kbps respectively, the degradation achieves less than 20 kbps. As well as in 2HCR protocol, the cause of different throughput degradation related to the hop number has been discussed in Section 2.3.

For 2-source multihop topologies, the end to end throughput for various hop number is illustrated in Figure 4-24. The maximum achievable throughput for each topology from 1-hop to 7-hop is 769 kbps, 447 kbps, 316 kbps, 280 kbps, 248 kbps, 218 kbps, and 200 kbps respectively. Compared to the throughput of the same hop topologies in 1-source networks, the throughput in 2-source topologies is lower, due to multisource collision. The high throughput degradation in this case happens when the hop number is increased from 1-hop topology into 2-hop and 3-hop, with the degradation achieves more than 130 kbps. For the rest of the hop rise, the degradation achieves less than 40 kbps

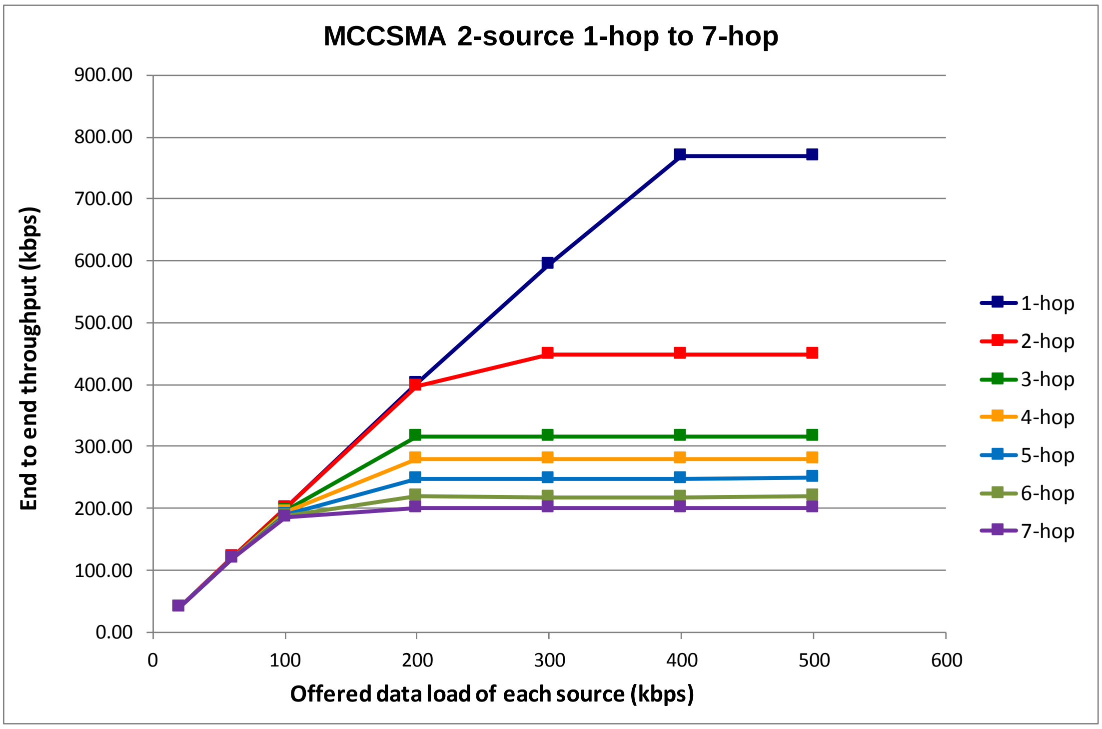

Figure 4-24 The end to end throughput of 2-source multihop networks with MC CSMA protocol

On the other hand, for the 3-source topologies, the end to end throughput of various hop numbers is illustrated in Figure 4-25. The maximum achievable throughput of each topology from 1-hop to 7-hop is 768 kbps, 447 kbps, 313 kbps, 276 kbps, 247, kbps, 217 kbps, and 194 kbps respectively. Similar with the 2-source topologies, the high throughput degradation occurs for the hop rise between 1-hop and 3-hop. The degradations in this case reaches more than 120 kbps.

Meanwhile, for the hop rise between 3-hop and 7-hop, the degradation reaches less than 40 kbps.

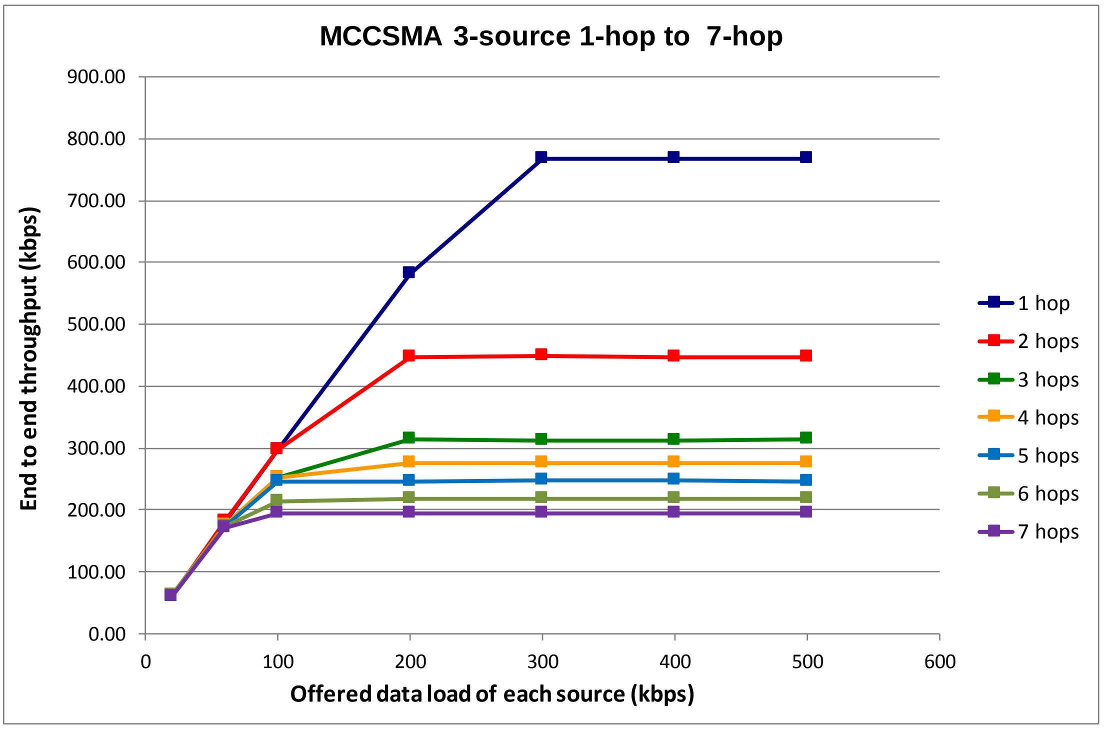

Figure 4-25 The end to end throughput of 3-source multihop networks with MC CSMA protocol

Furthermore, the simulation results for 1-source topologies with MC CSMA protocol enabling RTS/CTS is illustrated in Figure 4-26. From the figure, it can be seen that the throughput degradation is high if the chain topology is extended from 1-hop into 2-hop, 3-hop, and 4-hop. With the maximum throughput of each topology from 1-hop to 4-hop which is 587 kbps, 486 kbps, 319 kbps, and 177 kbps respectively, the degradation on each hop increase is more than 100 kbps with the highest degradation occurs when the hop number is risen from 2-hop into 3-hop. The throughput degradation for this case is 167 kbps. Contrary, the throughput degradation for the hop rise between 4-hop and 7-hop topologies is only 20 kbps and below, as the maximum throughput of each topology between 5-hop and 7-hop is 167 kbps, 148 kbps, and 134 kbps respectively. In addition, all maximum throughputs in this scenario are lower than the maximum throughputs with MC CSMA protocol disabling RTS/CTS.

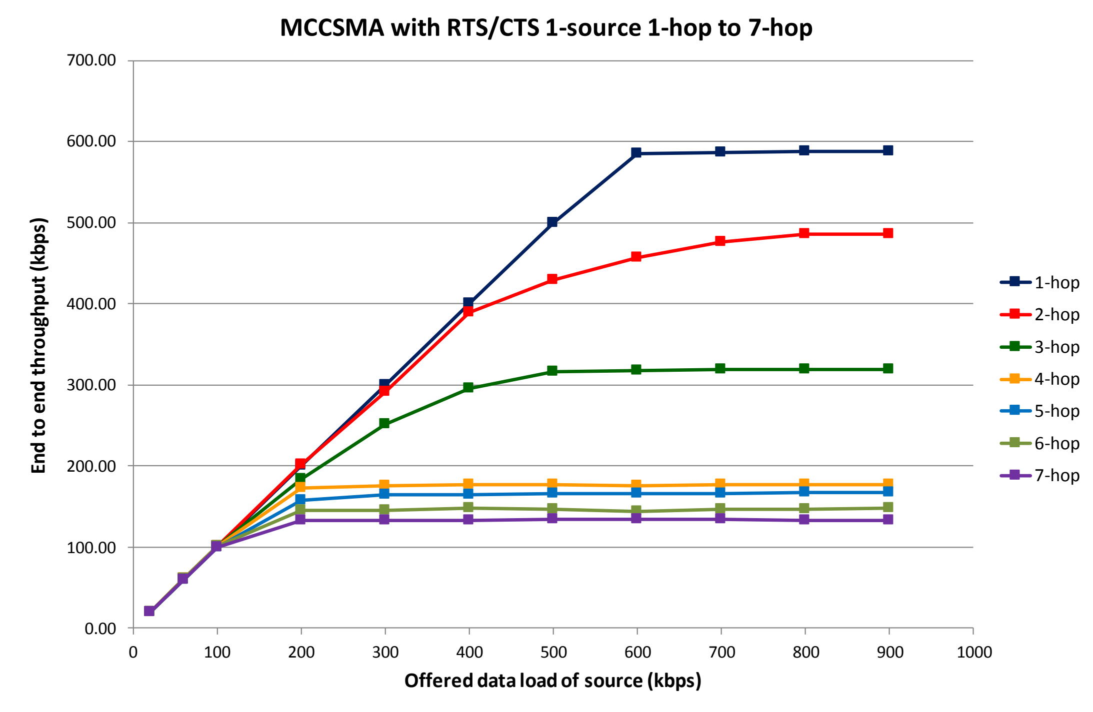

Figure 4-26 The end to end throughput of 1-source multihop networks with MC CSMA protocol enabling RTS/CTS

Moreover, the end to end throughput of 2-source multihop network with MC CSMA enabling RTS/CTS, is shown in Figure 4-27. The maximum achievable throughput for each topology between 1-hop to 7-hop networks, is 607 kbps, 377 kbps, 252 kbps, 175 kbps, 152 kbps, 133 kbps, and 117 kbps respectively. Excepted the throughput of 1-hop topology, all throughputs are lower than the throughputs of in 1-source for the same topology, due to multiple source collision. Meanwhile, the throughput of 2-source1-hop network which is slightly higher than the throughput of 1-source 1-hop network is possible affected by a multisource statistical gain. In case of throughout degradation, a significant degradation occurs between 1-hop and 4-hop topologies. The minimum degradation in these topologies is 7 kbps, which is obtained when 3-hop network is extended into 4-hop network. Beyond 4-hop network, the maximum degradation is only 23 kbps.

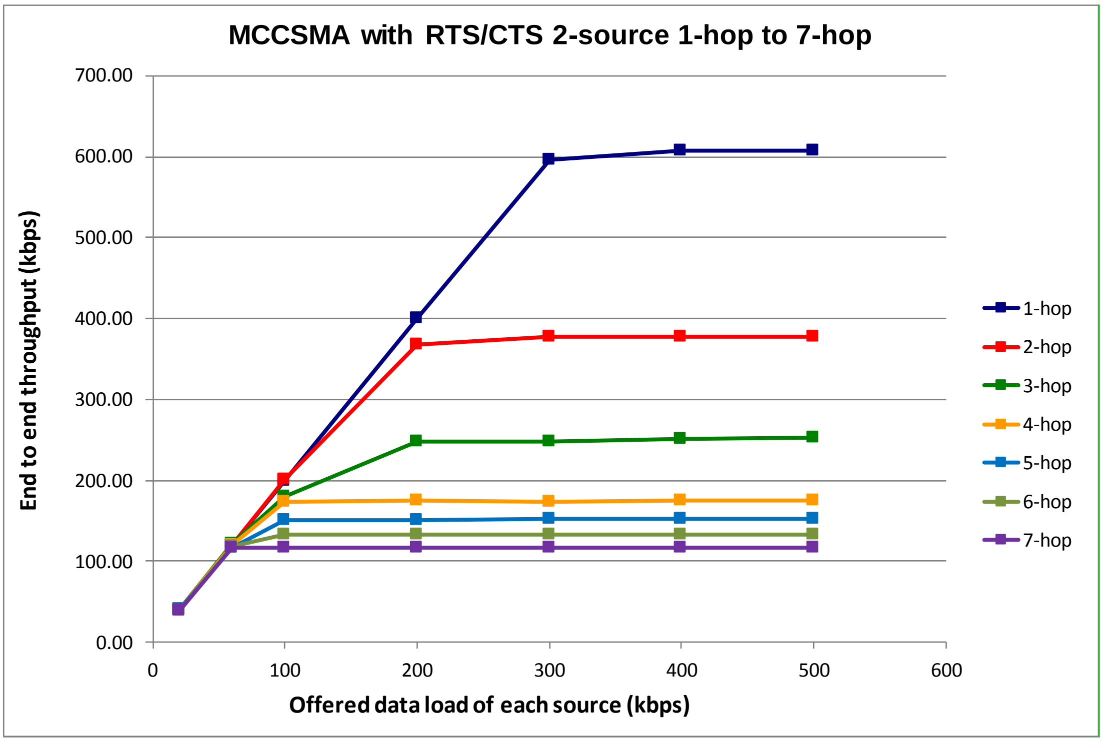

Figure 4-27 The end to end throughput of 2-source multihop networks with MC CSMA protocol enabling RTS/CTS

Finally, the throughput of 3-source multihop network is shown in Figure 4-28. The maximum achievable throughput of each topology between 1-hop and 7-hop in this case is 606 kbps, 369 kbps, 228 kbps, 167, kbps, 149 kbps, 131 kbps, and 116 kbps respectively. In comparison with the result in 2-source scenario, the throughput of the same topology in this 3-source scenario is lower. It indicates that an additional source has caused more packet collisions. Meanwhile, the highest throughput degradation, which is 237 kbps, is obtained when 1-hop topology is increased into 2-hop topology. The lowest degradation, on the other hand, is 15 kbps, which is obtained when 6-hop topology is extended into 7-hop topology.

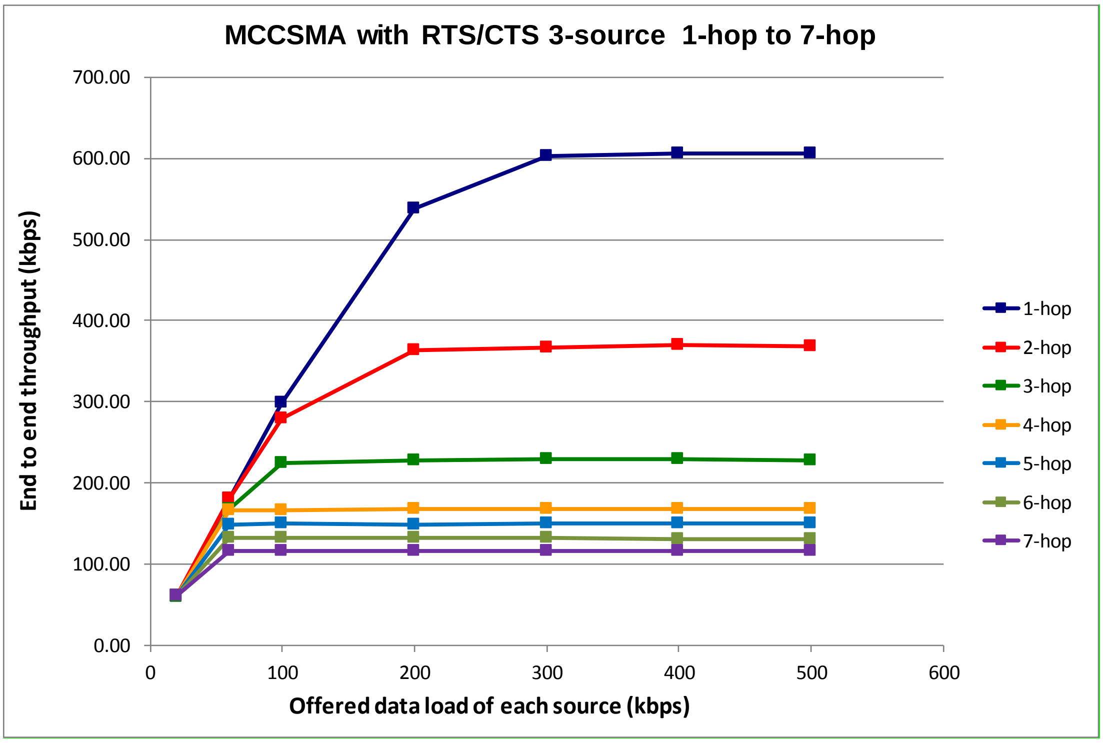

Figure 4-28 The end to end throughput of 3-source multihop networks with MC CSMA protocol enabling RTS/CTS

By referring to the throughputs of basic topologies denoted in 6 figures above, the estimation procedure can be undertaken for the 2-source and 3-source topologies shown by Figure 3-9 and 3-10 in Section 3-5. For 2-source 4-hop networks with shifted LH2 location, the comparison of the prediction and simulation result is denoted in Figure 4-29.

In case of LH2 connected to RN2, the predicted maximum throughput of 316 kbps and simulated throughput of 320 kbps give the deviation of 1.25 %. Concurrently, for LH2 connected to RN3, the deviation achieves 4.49 %, which is yielded from the predicted maximum throughput of 447 kbps and the simulated throughput of 468 kbps. This deviation is lower compared to the deviation in 2HCR topology for the same condition.

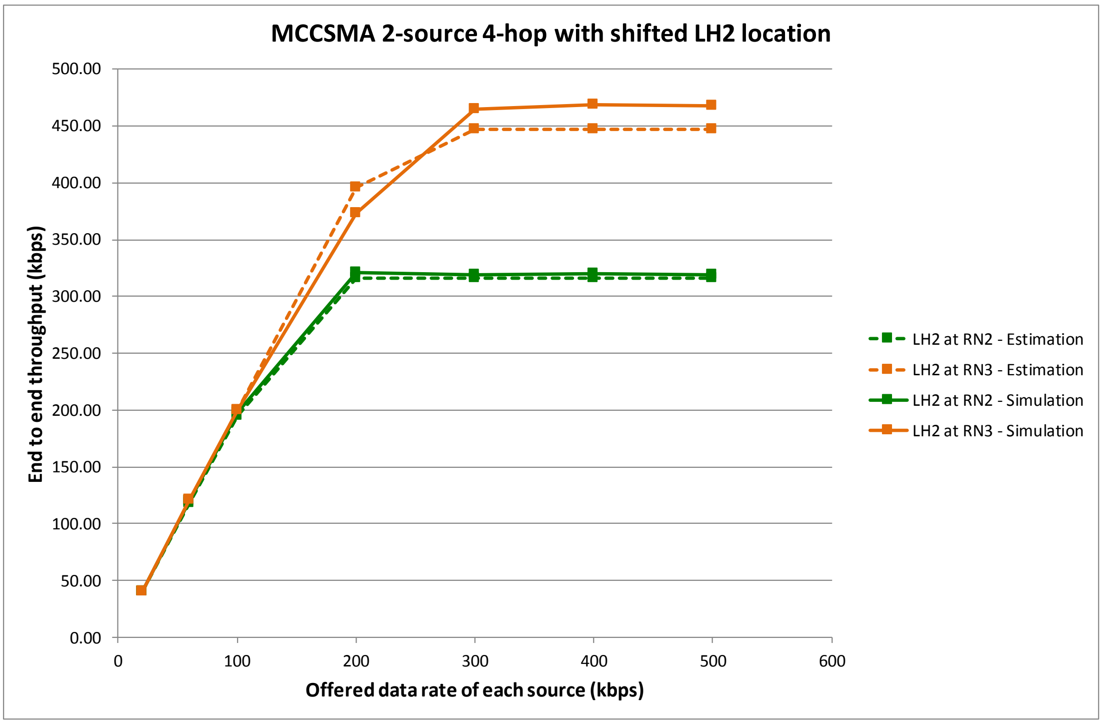

Figure 4-29 Comparison between estimation and simulation for 2-source 4-hop shifted LH2 location with MC CSMA protocol

Meanwhile, for 3-source 4-hop topologies with shifted LH3, the throughput of estimation and simulation result is illustrated in Figure 4-30. For the first scenario where LH3 is connected to RN2, the maximum deviation reaches 12.34 %, which is obtained from the predicted maximum throughput of 316 kbps and simulation throughput of 277 kbps. Meanwhile, if LH3 is connected to RN3, the maximum deviation achieves 6.29 %, for the predicted maximum throughput of 477 kbps and simulation throughput of 447 kbps.

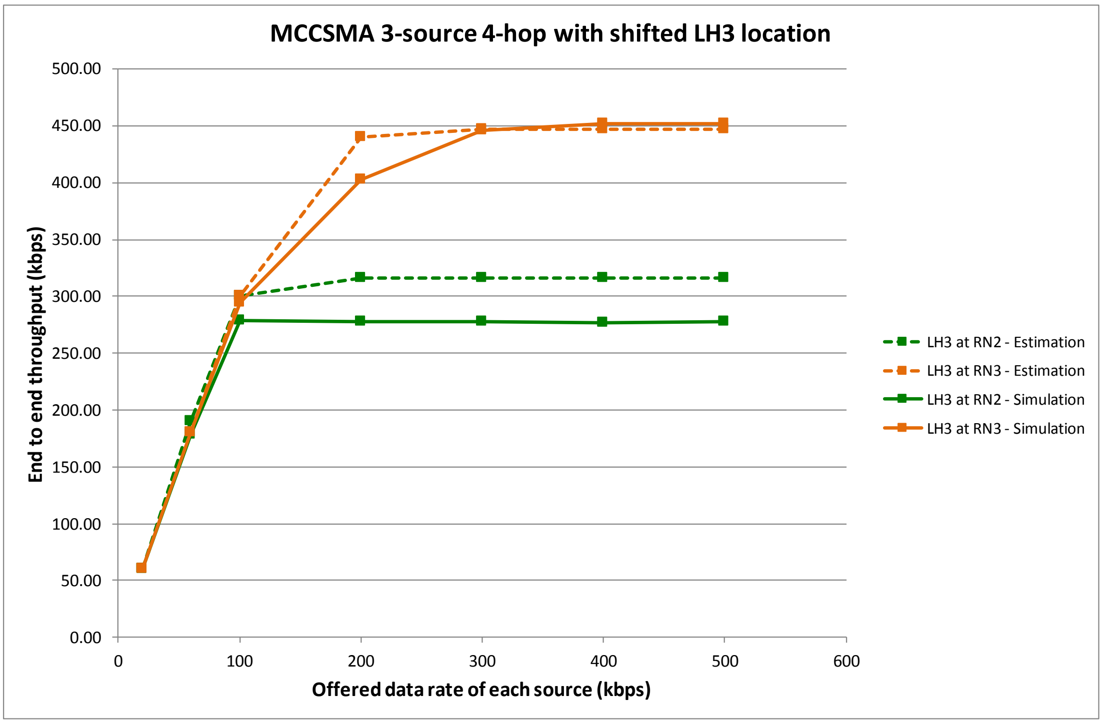

Figure 4-30 Comparison between estimation and simulation for 3-source 4-hop shifted LH3 location with MC CSMA protocol

If the chain is extended into 7-hop, the throughput of estimation and simulation methods for 2-source network with shifted LH2 location, is illustrated in Figure 4-31. The estimated maximum throughput for LH2 connected to RN2 topology, obtains 218 kbps, which is deviated only 0.46 % from the simulation result of 219 kbps. Meanwhile, the estimated maximum throughput for LH2 connected to RN3, obtains 248 kbps, which is deviated 4.44 % from the simulation result of 237 kbps. Again, these deviations are lower than the deviations in 2HCR protocol for the same topologies.

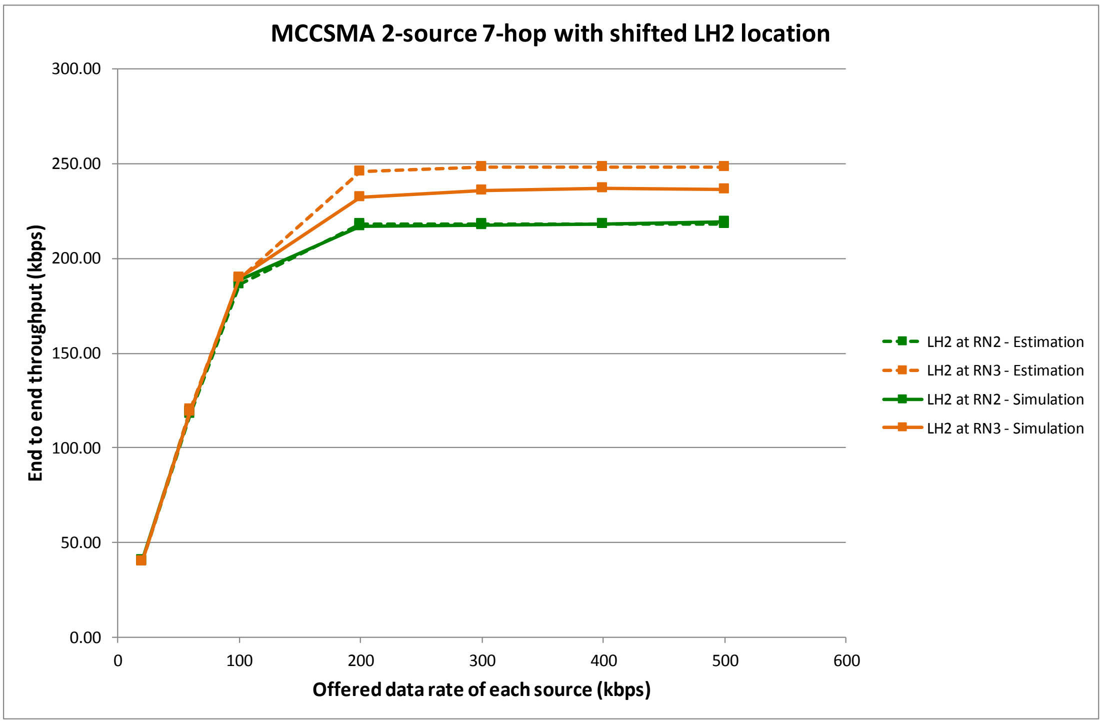

Figure 4-31 Comparison between estimation and simulation for 2-source 7-hop shifted LH2 location with MC CSMA protocol

Meanwhile, the comparison between the simulation and estimation of 3-source 7-hop networks is illustrated in Figure 4-32. The maximum deviation for topology with LH3 connected to RN2 achieves 1.38 % yielded from the estimated throughput of 218 kbps and simulated throughput of 215 kbps. On the other hand, the maximum deviation for topology with LH3 connected to RN3, achieves 6.05 % obtained from the estimated throughput of 248 kbps and simulated throughput of 233 kbps.

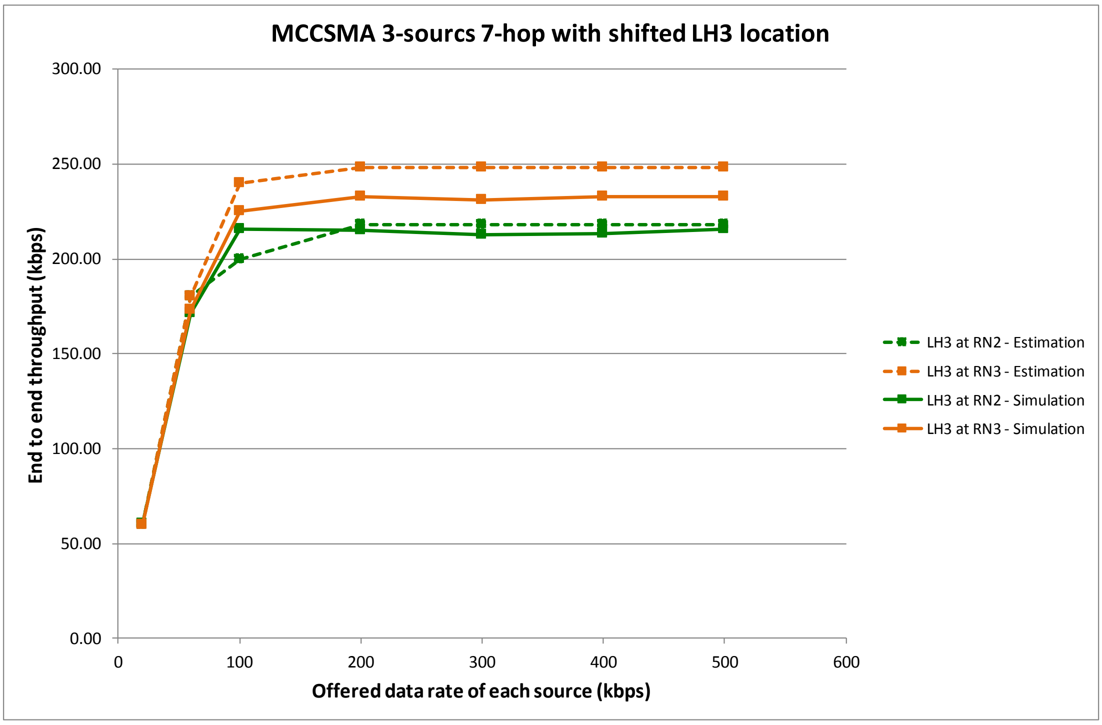

Figure 4-32 Comparison between estimation and simulation for 3-source 7-hop shifted LH3 location with MC CSMA protocol

Furthermore, as well as in 2HCR protocol, the prediction is also performed for MC CSMA protocol enabling RTS/CTS handshake. For 2-source 4-hop topologies, the comparison between estimation and simulation results is depicted in Figure 4-33. The estimated maximum throughput of 252 kbps and the simulated throughput of 256 kbps derive the deviation of 1.56 % for the topology with LH2 located near RN2. On the other hand, the estimated throughput of 377 kbps and the simulated throughput of 438 kbps derive the deviation of 13.93 % for the topology with LH2 connected to RN3. The deviation over 10 % yielded from this topology with 2HCR enabling RTS/CTS also occurs in MC CSMA protocol with the same conditions. It indicates that both the topology and RTS/CTS involvement are likely causing the high deviation.

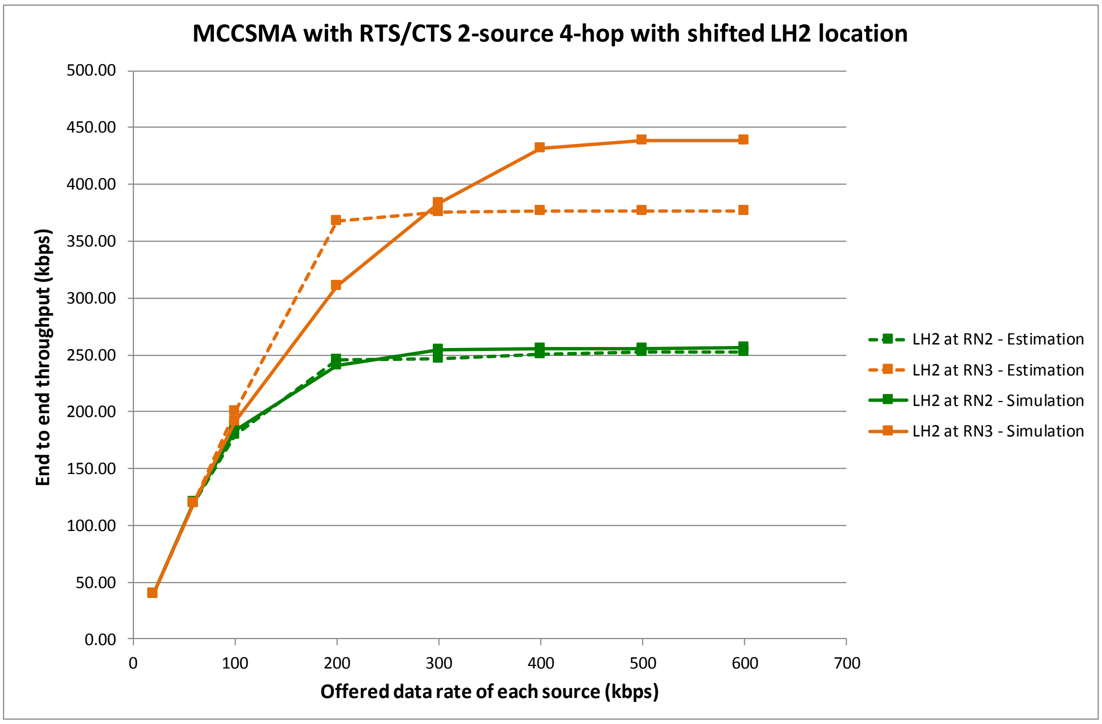

Figure 4-33 Comparison between estimation and simulation for 2-source 4-hop shifted LH2 location with MC CSMA protocol enabling RTS/CTS

Moreover, the comparison between prediction and simulation result for 3-source 4-hop network is depicted in Figure 4-34. The maximum deviation for the first scenario where LH3 located near RN2, achieves 6.75 % which is obtained from the prediction and simulation results of 252 kbps and 235 kbps respectively. Concurrently, the maximum deviation for the second scenario where LH3 located near RN3, achieves 16.41 % which is obtained from the prediction and simulation results of 377 kbps and 451 kbps respectively. Again, the high deviation occurred in 2HCR protocol also happens in MC CSMA with the same condition. However, the deviation in MC CSMA is less than the deviation in 2HCR protocol.

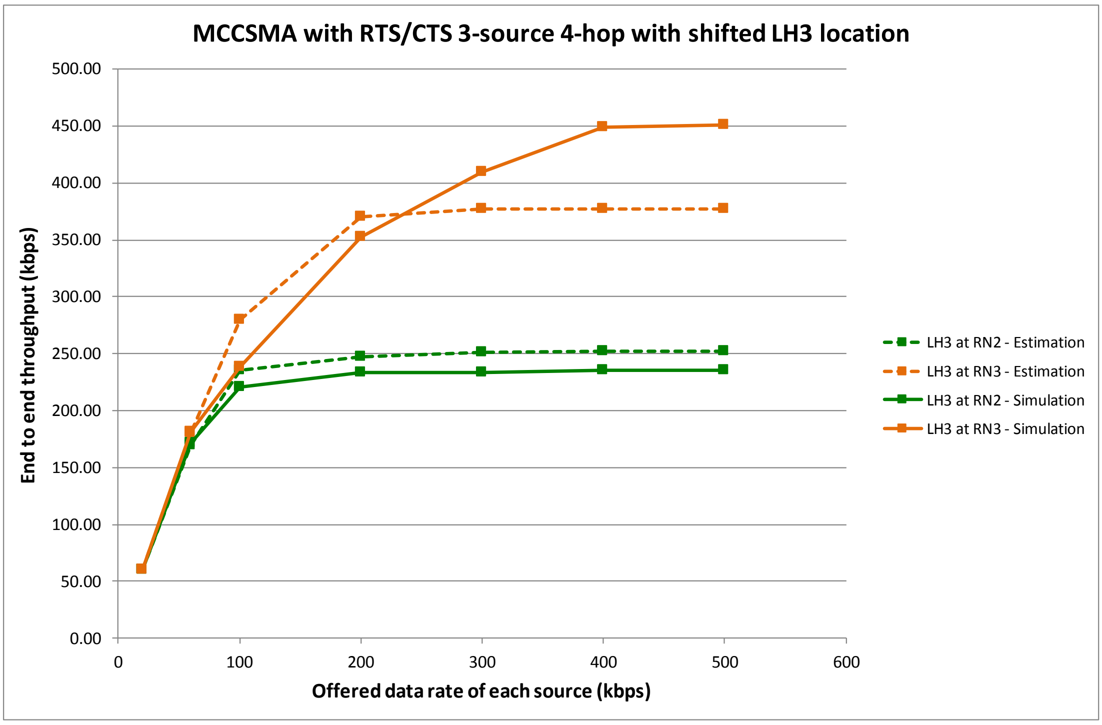

Figure 4-34 Comparison between estimation and simulation for 3-source 4-hop shifted LH3 location with MC CSMA protocol enabling RTS/CTS

If the chain length is increased into 7-hop, the estimation and simulation throughput of 2-source 7-hop network is depicted in Figure 4-35. The maximum throughputs yielded from the estimation and simulation of the topology with LH2 connected to RN2, are 133 kbps and 139 kbps respectively, causing the deviation of 4.32 % between the estimation and simulation results. Concurrently, the maximum achievable throughput obtained from the estimation and simulation of topology with LH2 connected to RN3, are 152 kbps and 160 kbps respectively derives the deviation of 5.00 % between the simulation and simulation throughputs. Both deviations are below 10 %, indicating that such unexpected behaviour happening in previous topologies is likely not affecting the throughput of these 2-source 7-hop topologies.

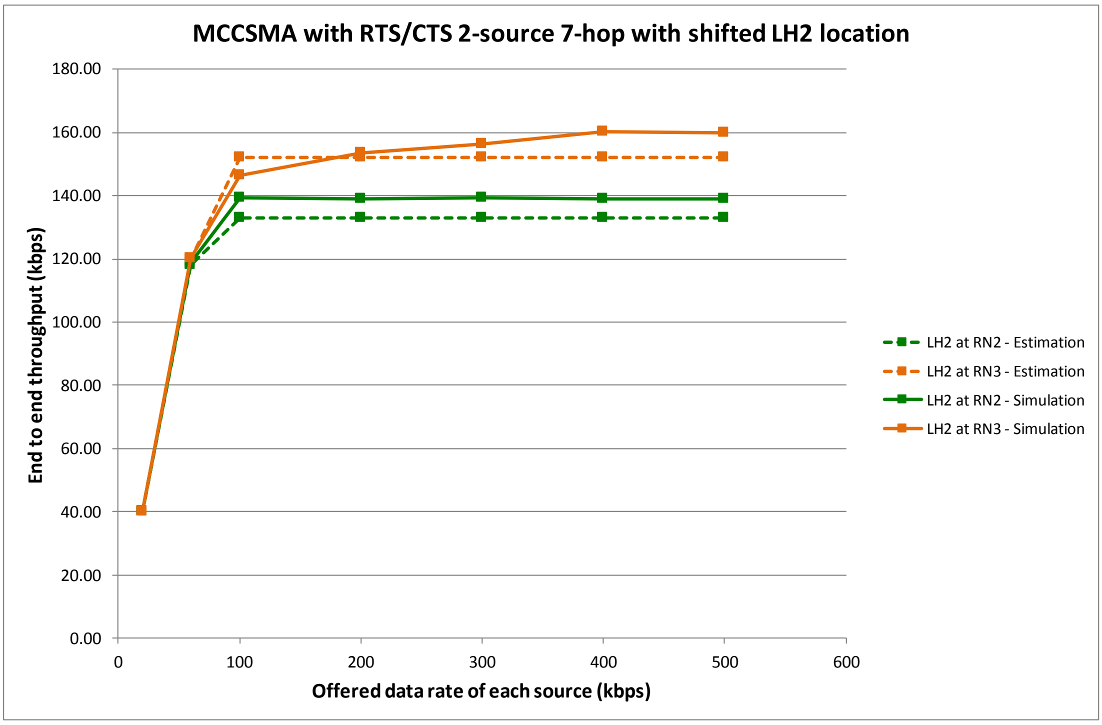

Figure 4-35 Comparison between estimation and simulation for 2-source 7-hop shifted LH2 location with MC CSMA protocol enabling RTS/CTS

Finally, the comparison between the prediction and simulation for 3-source 7-hop network is depicted in Figure 4-36. For the first scenario where LH3 is located near RN2, the estimated maximum throughput is 133 kbps, which is deviated 7.64 % from the simulated throughput of 144 kbps. Meanwhile, for the second scenario where LH3 is located near RN3, the estimated throughput is 152 kbps, which is deviated 9.52 % from the simulated maximum throughput that is 168 kbps. Although these deviations are higher than in 2-source 7-hop case, they are still below 10 %.

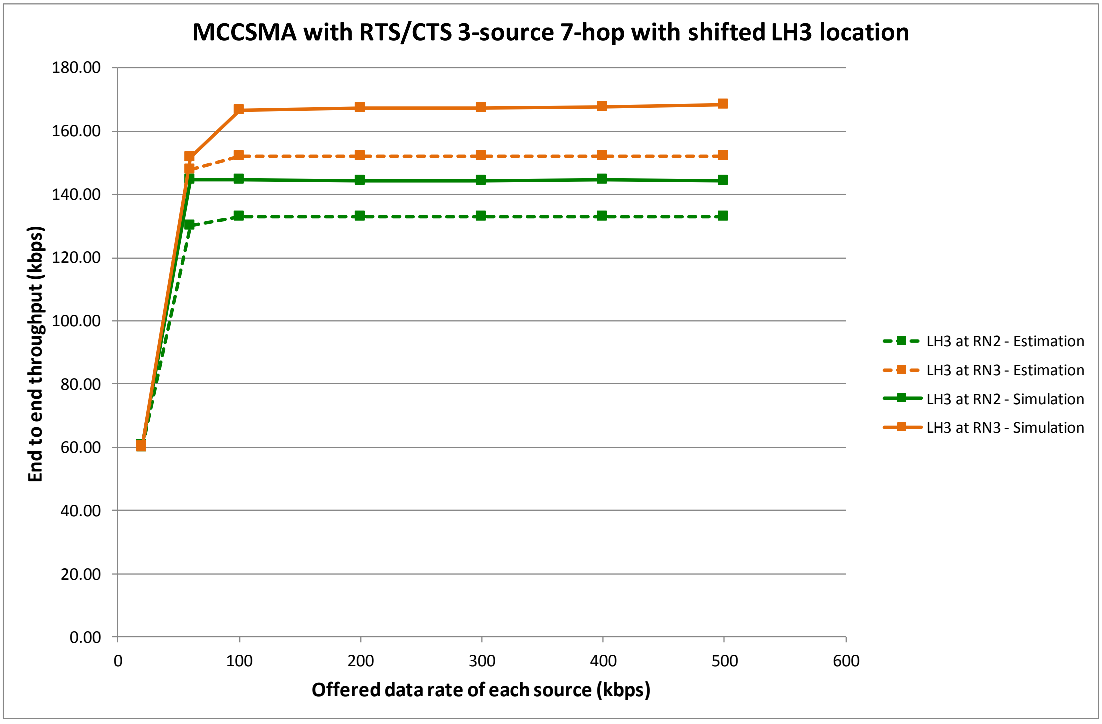

Figure 4-36 Comparison between estimation and simulation for 3-source 7-hop shifted LH2 location with MC CSMA protocol enabling RTS/CTS

In conclusion, most predictions reach the maximum deviation less than 10 %. Among sixteen prediction results, three of them obtain the maximum deviation which is higher than 10 %. The two highest deviations are derived from the same topology as in 2HCR with the protocol enabling RTS/CTS. These two topologies are 2-source 4-hop with LH2 connected to RN3, and 3-source 4-hop with LH3 connected RN3. The cause of this high deviation has been addressed in previous section. In addition, the average maximum deviation of MC CSMA protocol is 6.04 % which is lower than the average deviation of 2HCR protocol. Thus, the estimation results in MC CSMA are more accurate than in 2HCR.

4.5 EVALUATION OF THE ESTIMATION MODELS FOR COMPLEX NETWORKS WITH 802.11b

The evaluation of the estimated throughputs for 2 channels protocols has been provided in section 4.3 and 4.4. To evaluate the estimated result for 1 channel protocol, the examination is performed for 802.11b. Before providing estimation, the simulation to obtain the throughput of basic topologies has been conducted with the results as follows. As the same as two previous protocols, the simulation with 802.11b protocol is performed in both disabled and enabled RTS/CTS. For 1-source multihop topologies with 802.11b protocol disabling RTS/CTS, the end to end throughputs for various topologies are illustrated in Figure 4-37.

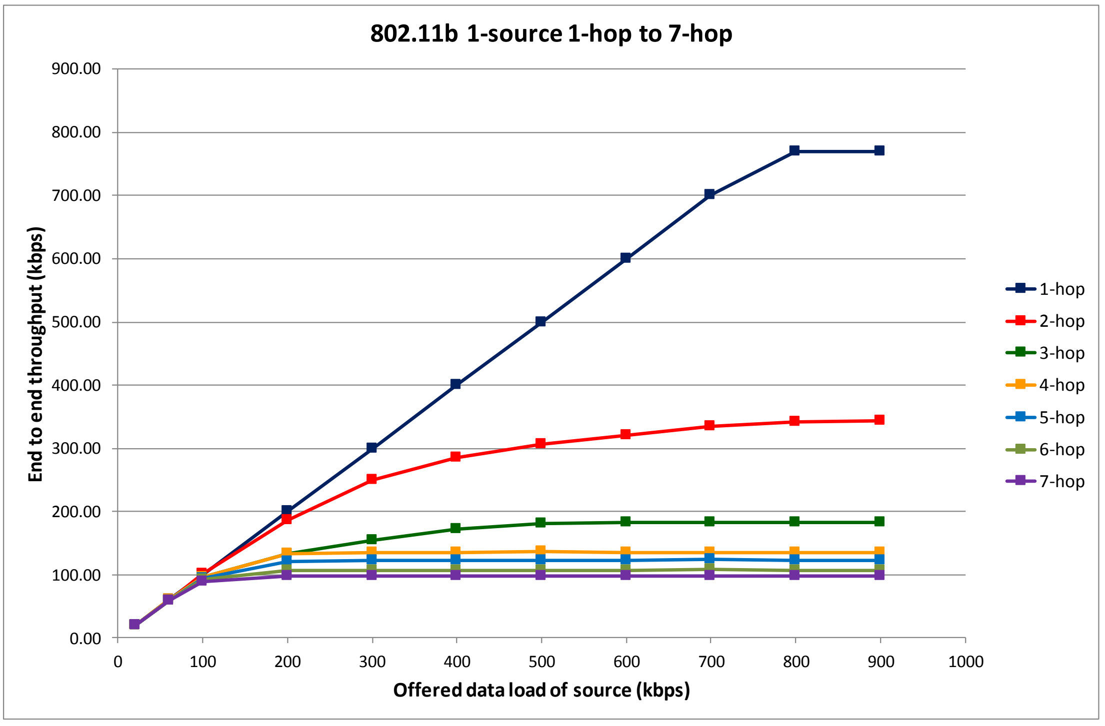

Figure 4-37 The end to end throughput of 1-source multihop networks with 802.11b protocol

It is shown in Figure 4-37 that the end to end throughput of 1-hop topology is the same as the offered data rate for up to 700 kbps. However, the throughput then stays at 770 kbps for the offered data rate of 800 kbps and 900 kbps. Compared with the results in 2HCR and MC CSMA for the same topology, it can be seen that the throughput of 1-hop topology with 802.11b is the same. This is because the use of different protocols has not given a significant impact for 1-hop throughput. However, if the chain is extended into 2-hop, 3-hop and 4-hop, the throughput reduces significantly. With the maximum throughput of 342 kbps, 182 kbps, and 135 kbps for 2-hop, 3-hop, and 4-hop respectively, the throughput degradation between 1-hop to 4-hop is higher than 40 kbps.

On the other hand, the maximum throughputs of 5-hop, 6-hop, and 7-hop topologies are 123 kbps, 107 kbps, and 98 kbps respectively. Through such results, it is denoted that the throughput degradation between 4-hop and 7-hop is less than 20 kbps. In addition, it is also found that the maximum throughputs of all topologies, excepted 1-hop, are lower than in MC CSMA and 2HCR protocols as this 802.11b protocol use only a single channel.

Furthermore, the throughput of 2-source network with various chain lengths is depicted in Figure 4-38. For 1-hop topology, the end to end throughput is the same as the offered data rate for the individual source data rate up to 300 kbps. Beyond this individual rate the throughput cannot achieve the same data rate generated by the sources, and stays at the maximum throughput of 766 kbps. Compared with 1-source 1-hop topology, the maximum achievable throughput of 2-source 1-hop topology is 4 kbps lower. This is most possibly caused by the multisource collision.

Concurrently, the high throughput declination occurs between 1-hop and 4-hop network. With the throughput of 290 kbps for 2-hop network, 167 kbps for 3-hop network, and 130 kbps for 4-hop network, it can be calculated that the throughput declination between 1-hop to 4-hop is more than 35 kbps. The highest declination which is 476 kbps occurs when 1-hop topology is extended into 2-hop topology. On the other hand, with the maximum throughput of 105 kbps for 5-hop network, 96 kbps, for 6-hop network, and 89 kbps for 7-hop network, the throughput declination between 4-hop and 7-hop is below 30 kbps.

Figure 4-38 The end to end throughput of 2-source multihop networks with 802.11b protocol

Moreover, the throughput of 3-source network with various hop numbers is shown in Figure 4-39. The maximum achievable throughput of each topology from 1-hop to 7-hop is 766 kbps, 290 kbps, 167 kbps, 130 kbps, 105 kbps, 96 kbps, and 88 kbps respectively. As well as in 1-source and 2-source topologies, the maximum throughput declines with the increase of the chain length. The highest declination is 476 kbps, which is obtained by increasing the chain from 1-hop into 2-hop. However, more additional hop number will reduce the throughput declination as well as the maximum achievable throughput. The lowest declination is 8 kbps, which is found by increasing the chain from 6-hop into 7-hop.

In addition, all maximum achievable throughputs of 3-source topologies are similar with the maximum achievable throughput of 2-source topologies. These results indicate that more multisource collisions due to the third source do not impact the network throughput. It is possibly because the additional packets sent by the third source collide with the packets from the first and second sources which are already in collision.

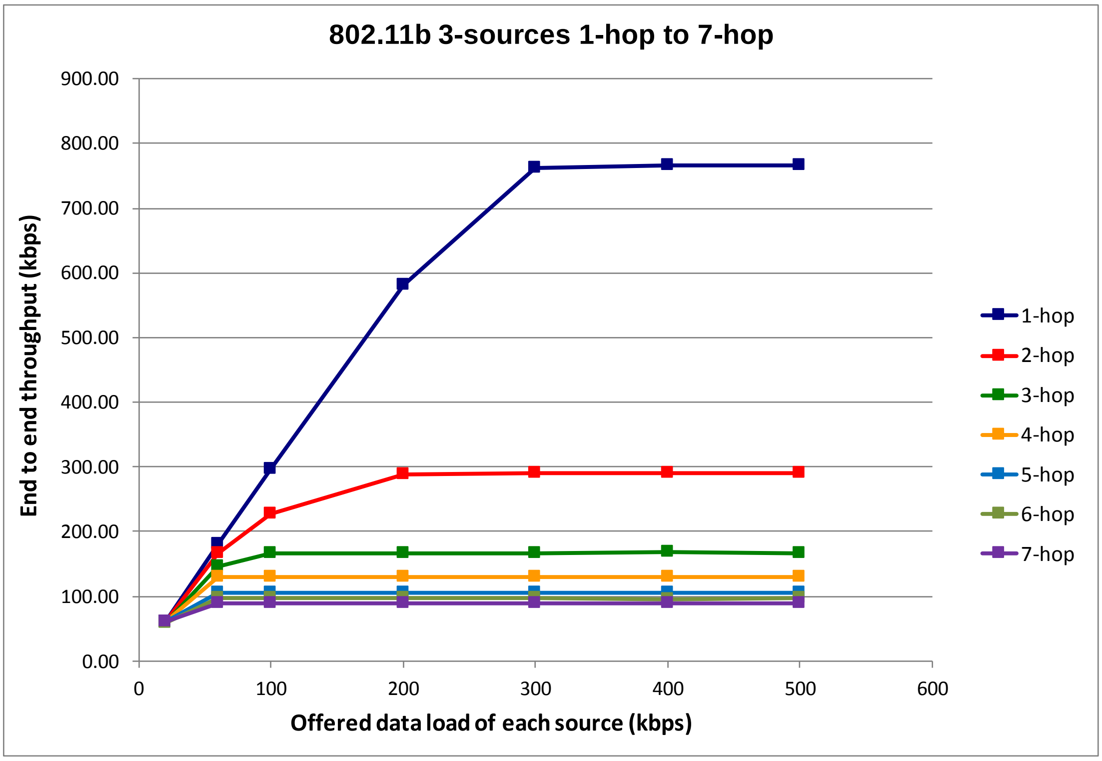

Figure 4-39 The end to end throughput of 3-source multihop networks with 802.11b protocol

As it has been mentioned in the earliest paragraph of this section, the simulation is also undertaken for 802.11b protocol enabling RTS/CTS handshake. With this condition, the throughput of 2-source multihop topologies for various hop numbers is depicted in Figure 4-40. The maximum throughput for each topology from 1-hop to 7-hop is 583 kbps, 265 kbps, 167 kbps, 121 kbps, 107 kbps, 93 kbps, and 86 kbps respectively. Such results are below the throughputs of the same topologies with 802.11b protocol disabling RTS/CTS. This lower throughput is impacted by the presence of RTS and CTS packets that contend with the data packets, particularly for the higher input data rate sent by the source. For the packet size used in this simulation which is only 2000 bits length, the RTS and CTS packets size becomes a high cost overhead. This problem has been addressed in Section 2.3, where the degradation factors of a multihop network are discussed.

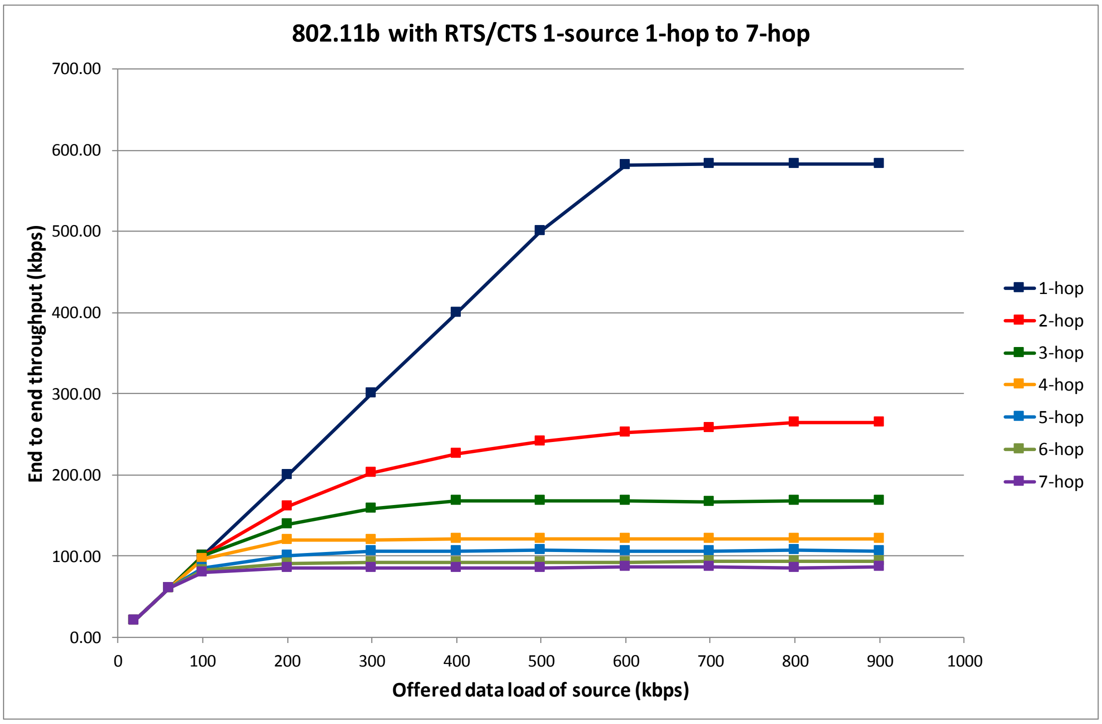

Figure 4-40 The end to end throughput of 1-source multihop networks with 802.11b protocol enabling RTS/CTS

Moreover, the end to end throughput of 2-source multihop network with various hop number is shown in Figure 4-41. The maximum throughput of each topology from 1-hop to 7-hop achieves 602 kbps, 223 kbps, 158 kbps, 128 kbps, 103 kbps, 93 kbps, and 85 kbps. Excepted the maximum throughput of 1-hop topology, the maximum throughputs of all topologies are lower than these of 1-source case, due to the multisource collision. However, the maximum throughput of 1-hop topology in 2-source network is higher than in 1-source network. It could be due to the statistical gain of multisource network. Meanwhile, in case of throughput degradation, the rise of hop numbers from 1-hop to 2-hop causes the highest degradation which is 379 kbps. In contrast, the lowest degradation is only 8 kbps which is derived on chain extension from 6-hop into 7-hop.

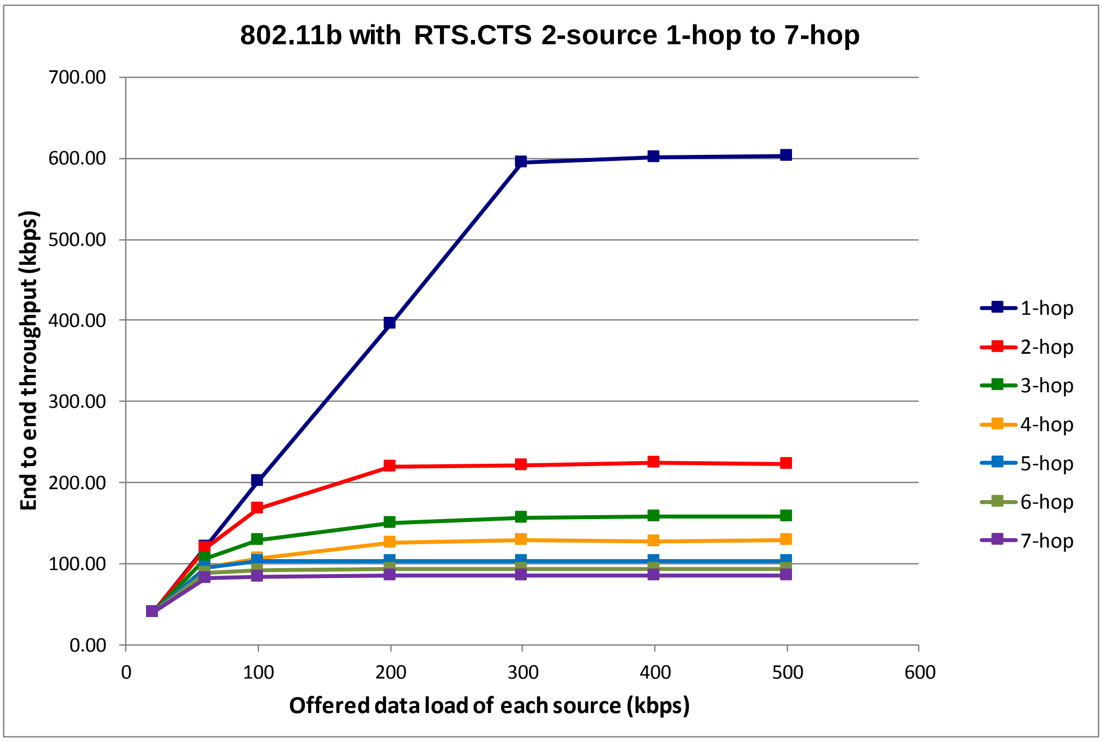

Figure 4-41 The end to end throughput of 2-source multihop networks with 802.11b protocol enabling RTS/CTS

Finally, the throughput of 3-source topologies with various hop numbers is depicted in Figure 4-42. To compare with the result of 2-source multihop network, the throughput of each topology of 3-source network is as follows. For 1-hop topology the maximum throughput of 1-hop topology is 602 kbps, which is the same with the throughput of 2-source case. The same throughput may indicate that the packets from the third source arrive at the time where packets from the other two sources are already collided. On the other hand, with the maximum throughput of 215 kbps, 145 kbps, 125 kbps, 103 kbps, 92 kbps, and 83 kbps, for 2-hop to 7-hop topologies respectively, it is shown that all throughputs are below the maximum throughputs of 2-source case. As such, the packets generated by the third source are likely increasing the multisource collision that impact to the throughput declination. Furthermore, it is also found that the highest throughput degradation due to the increase of hop number, is 387 kbps which is obtained when 1-hop topology is extended into 2-hop. The lowest degradation, on the other hand, is 9 kbps which is yielded when 6-hop topology is extended into 7-hop.

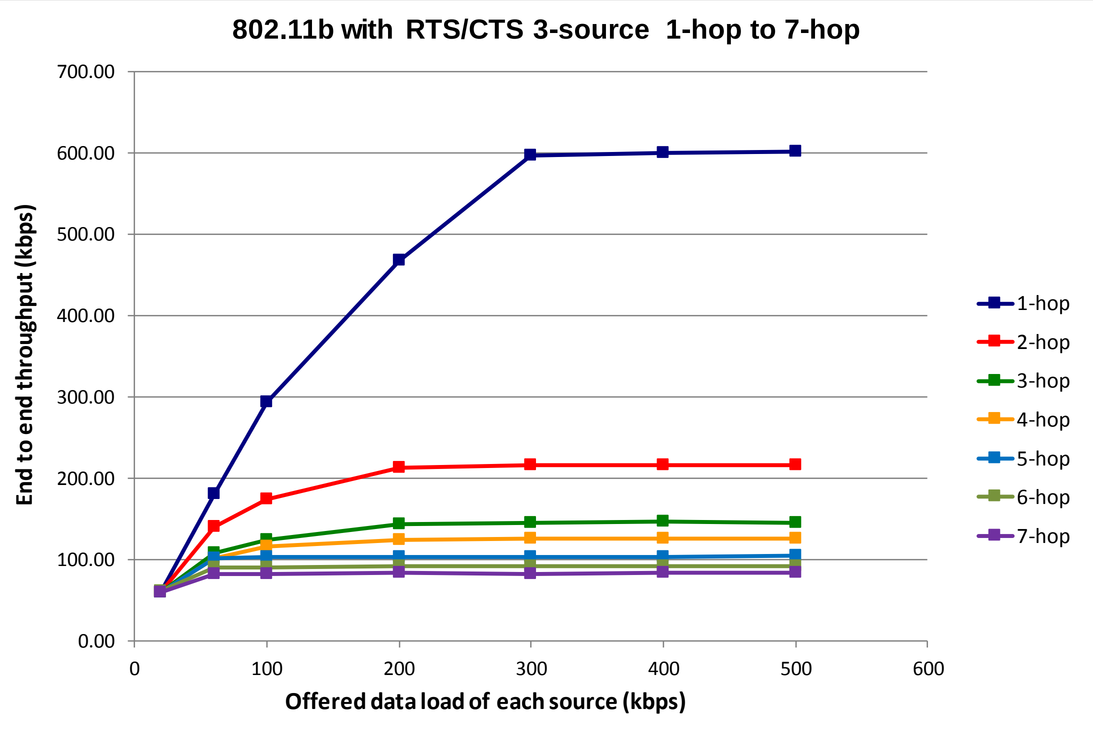

Figure 4-42 The end to end throughput of 3-source multihop networks with 802.11b protocol enabling RTS/CTS

By means of the throughputs of the basic topologies obtained from the simulations as presented above, an estimation procedure has been undertaken for 2-source and 3-source topology as depicted by Figure 3-9 and 3-10 in Section 3-5. For 2-source 4-hop topologies with shifted LH2 location, the throughput of the estimation and the simulation result is shown in Figure 4-43. The estimated maximum throughput of network with LH2 connected to RN2 is 166 kbps, while the simulation result gives the maximum throughput of 180 kbps. Therefore, the maximum deviation becomes 7.78 %, which is less than 10 %. On the other hand, with the estimated maximum throughput of 288 kbps, and the simulated throughput of 301 kbps, the maximum deviation of network with LH2 connected to RN3 achieves 4.32 %. Unlike the results in 2HCR and MC CSMA, the estimation of the network with LH2 connected to RN3 is more accurate than the estimation of network with LH2 connected to RN2.

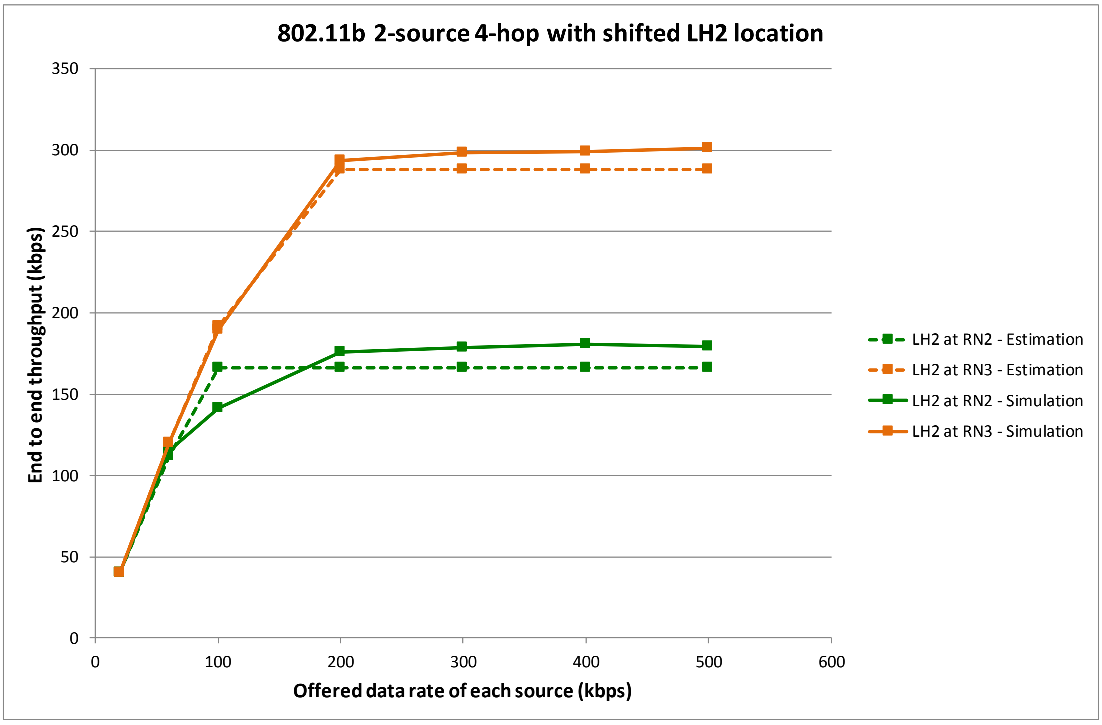

Figure 4-43 Comparison between estimation and simulation for 2-source 4-hop shifted LH2 location with 802.11b protocol

Concurrently, the throughput of the estimation and the simulation for 3-source 4-hop network with shifted LH3 location is shown in Figure 4-44. For the network with LH3 connected to RN2, the maximum throughput obtained from the estimation is 166 kbps, which is deviated 10.24 % from the simulation result with the maximum throughput of 149 kbps. On the other hand, with source LH3 is connected RN3, the estimated maximum throughput achieves 288 kbps. This result is deviated 2,37 % from the simulation result with the throughput of 295 kbps. With the deviation of the first scenario (ie. one source is connected to RN2) is higher than the deviation of the second scenario (ie. one source is connected to RN3), the estimation results of 3-source 4-hop follows the result in 2-source 4-hop. However, this does not match with the trend in most of estimation results in 2HCR and MC CSMA protocols.

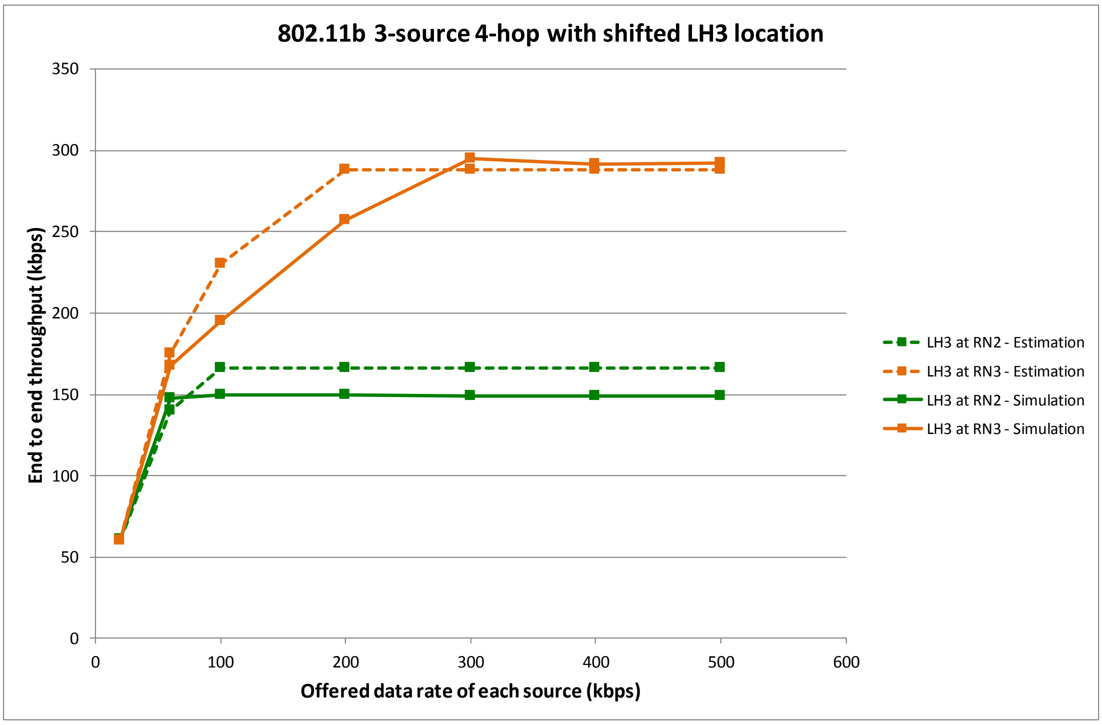

Figure 4-44 Comparison between estimation and simulation for 3-source 4-hop shifted LH3 location with 802.11b protocol

Furthermore, the comparison between the simulation and the prediction result of 2-source 7-hop topologies with shifted LH2 location is illustrated in Figure 4-45. The predicted maximum throughput of the topology with LH2 connected to RN2 is 95 kbps. With such throughput, the deviation of this topology reaches 4.21 % as the maximum throughput yielded from the simulation is 91 kbps. On the other hand, when LH2 is connected to RN3, the predicted maximum throughput obtains 105 kbps. By this result, the maximum deviation achieves 9.52 % as the maximum throughput obtained from the simulation is 95 kbps. With the deviation of the first scenario lower than the second scenario, the estimation results for 2-source 7-hop topology does not follow the trend of previous two topologies, however, it matches with the general trend of most topologies in 2HCR and MC CSMA protocols.

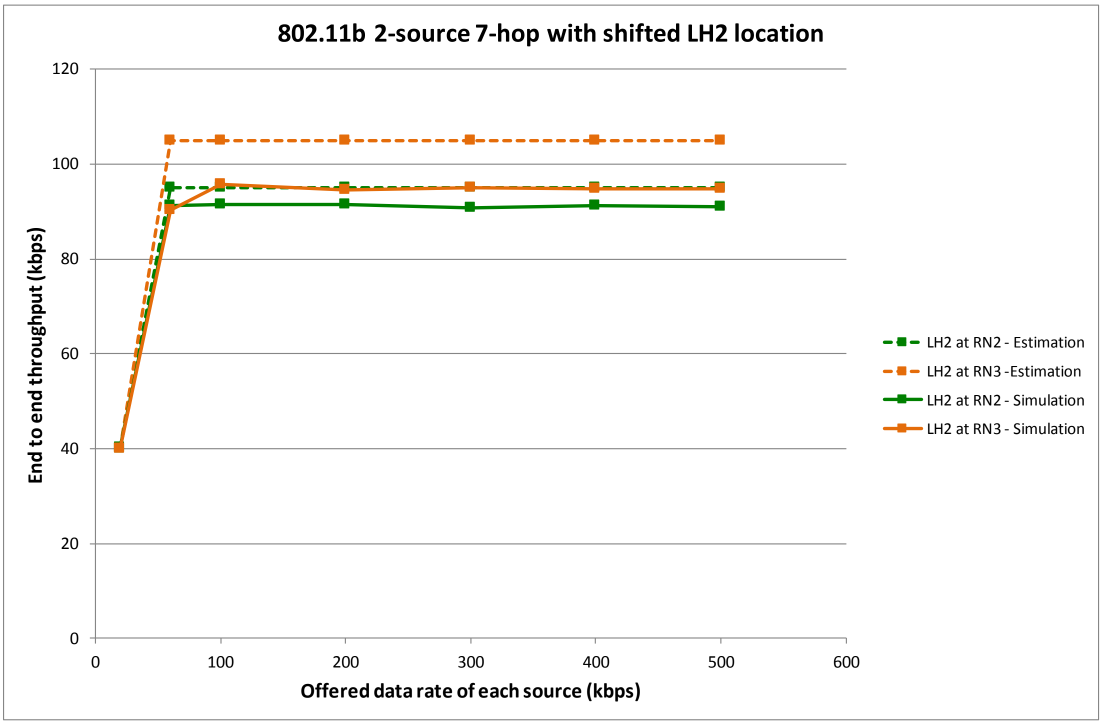

Figure 4-45 Comparison between estimation and simulation for 2-source 7-hop shifted LH2 location with 802.11b protocol

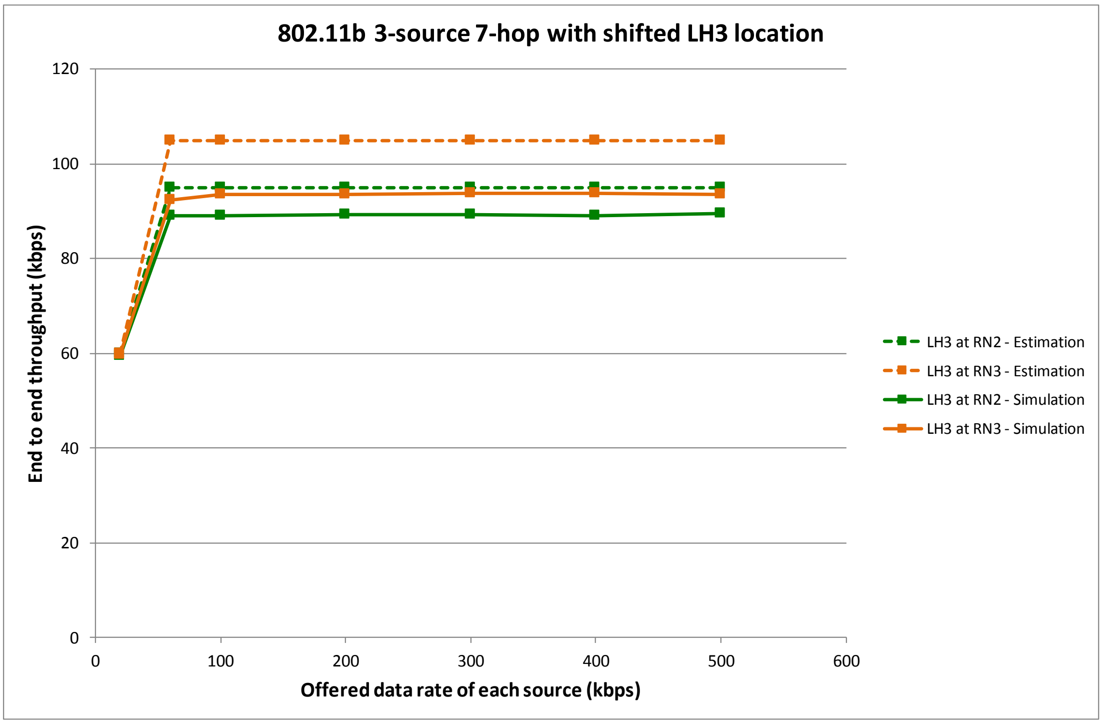

Figure 4-46 Comparison between estimation and simulation for 3-source 7-hop shifted LH3 location with 802.11b protocol

Moreover, for 3-source 7-hop network, the throughputs obtained from the estimation and simulation are depicted in Figure 4-46. For the first scenario where LH3 is connected to RN2, the estimated maximum throughput derives 95 kbps whilst the simulated throughput achieves 89 kbps. Therefore, the maximum deviation becomes 6.32 %. On the other hand, for the second scenario where LH3 is connected to RN3, the estimated throughput obtains 105 kbps, whereas the simulation obtains the throughput of 93 kbps. As such, the maximum deviation for this scenario achieves 11.43 % which is higher than the limit of 10 %.

While the evaluation of estimated throughput above is provided with 802.11b protocol without involving RTS/CTS handshake, the following evaluation is undertaken with 802.11b protocol enabling RTS/CTS. The first evaluation is performed for 2-source 4-hop topologies with LH2 shifted location. The throughput comparison between the estimation and simulation results is shown in Figure 4-47.

Figure 4-47 Comparison between estimation and simulation for 2-source 4-hop shifted LH2 location with 802.11b protocol enabling RTS/CTS

For the topology with LH2 is connected to RN2, the predicted maximum throughput derives 158 kbps, which is deviated 17.08 % from the simulation result with the throughput of 131 kbps. On the other hand, if LH2 is connected to RN3, the predicted maximum throughput derives 223 kbps, which is deviated 12.55 %. Both predicted throughputs show the deviation that is higher than 10 %. Again, an expected behaviour in the simulation cannot be covered by this simple estimation procedure.

Concurrently, for 3-source 4-hop topologies with shifted LH3 location, the comparison between the estimation and the simulation results is illustrated in Figure 4-48. If LH3 is located near RN2, the maximum throughput obtained by the simulation and the estimation is 126 kbps and 158 kbps respectively. For these throughputs, the deviation between the simulation and estimation is 20.25 %. Meanwhile, if LH3 is located near RN3, the maximum achievable throughput derived by the simulation and the estimation is 257 kbps and 221 kbps. And thus, the deviation between them is 14.01 %. The high deviation occurred in 2-source 4-hop topologies also happens in 3-source 4-hop topologies.

Figure 4-48 Comparison between estimation and simulation for 3-source 4-hop shifted LH3 location with 802.11b protocol enabling RTS/CTS

Furthermore, the comparison between the prediction and the simulation result for 2-source 7-hop topologies with shifted LH2 location, is depicted in Figure 4-49. For the first topology with LH2 is connected to RN2, the maximum throughput obtained from the estimation is 93 kbps, which is 13.98 % higher than the simulation result with 80 kbps. On the other hand, for the second topology with LH2 is connected to RN3, the maximum throughput yielded by the estimation is 103 kbps, which is 20.39 % higher than the simulation result with 82 kbps. The high deviation estimation results still occur in this 2-source 7-hop topology.

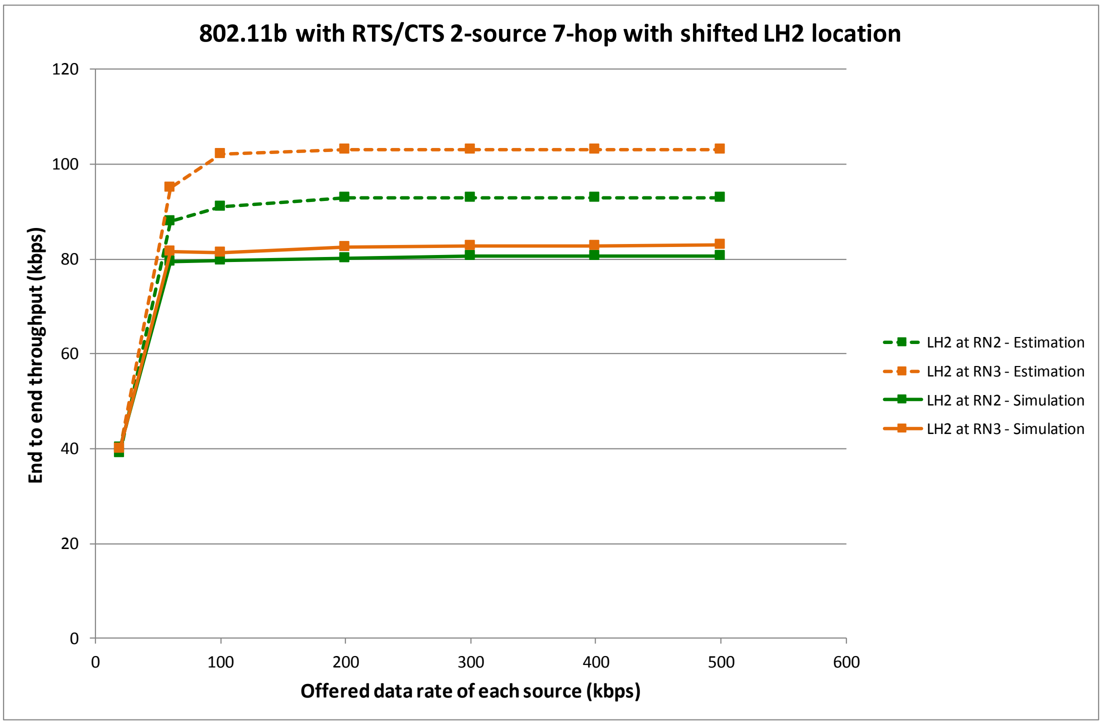

Figure 4-49 Comparison between estimation and simulation for 2-source 7-hop shifted LH2 location with 802.11b protocol enabling RTS/CTS

Finally, the comparison between the estimation and the simulation results is illustrated in Figure 4-50. With the estimated maximum throughput of 93 kbps and the simulated throughput of 80 kbps, for LH3 connected to RN2, the deviation becomes 13.98 %. Meanwhile, with the estimated maximum throughput of 103 kbps and the simulated maximum throughput of 82 kbps, for LH3 connected to

RN3, the deviation achieves 20.39 %. Again, the high deviation estimation result also occurs in 3-source 7-hop topologies.

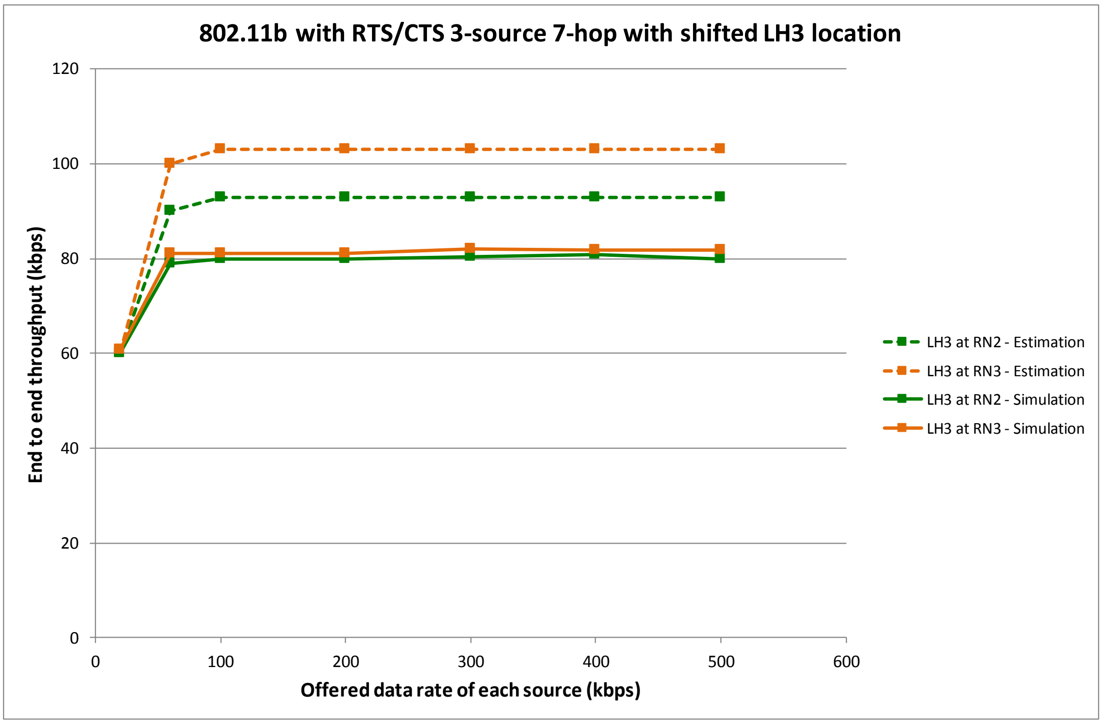

Figure 4-50 Comparison between estimation and simulation for 3-source 7-hop shifted LH3 location with 802.11b protocol enabling RTS/CTS

In conclusion, it has been observed that most estimation results for network throughput with 802.11b protocol without involving RTS/CTS achieve the deviation less than 10 %. It indicates that the estimation throughput is quite accurate. However, the opposite results occur when RTS/CTS handshake is enabled. Under such condition, all estimation results achieve higher deviations with the range between 12.55 % and 20.39 %. Referring to the explanation in Section 4.3, the decomposition process of estimation method that does not involve the correlation of entire network could be the case of inaccuracy of this method. In addition, the average maximum deviation of estimation in 802.11b protocol reaches 11.80 %.

4.6 SUMMARY

This chapter has discussed an estimation method to predict the throughput of the complex network. The procedure is provided by mixing the empirical and analytical methods as explained in Section 4.2. In general, the procedure is undertaken by decomposing the complex network into subnetworks that are identical with the structure in basic topologies. The predicted throughput then is obtained by an iterative process.

The accuracy of this prediction method is examined by comparing the estimation result with the result of simulation of a targeted complex network. The examination is provided for 2HCR, MC CSMA, and 802,11b protocols to obtain the accuracy of throughput estimation for network working under each protocol. For 2HCR and MC CSMA, despite of some estimations achieving more than 10 % maximum deviation, most of deviations are less than 10 %, which indicate that the estimation results are quite accurate. However, for 802.11b, most of estimations provide the deviation below 10 % if RTS/CTS packets are not employed. Contrary, all estimations obtain the deviation higher than 10 % if RTS/CTS handshake is enabled.

According the explanation in Section 4.3, it seems that the decomposition process that does not consider the correlation of entire network could be the cause of the estimation accuracy. While the impact of such decomposition process does not significantly affect the accuracy of estimation in 2HCR and MC CSMA protocols, also 802.11b protocol without involving RTS/CTS, the estimation in 802.11b protocol with RTS/CTS, in contrast, is significantly affected by this simple decomposition process.

CHAPTER 5

BIDIRECTIONAL TRAFFIC AND PRIORITY SUPPORT

5.1 INTRODUCTION

Chapter 3 has addressed the performance of 2HCR in a unidirectional traffic where traffic flows only from sensor nodes (SNs) to control station (CS), which is in this thesis referred as forward traffic. In this chapter, we consider the bidirectional traffic scenario where an additional traffic, i.e., reverse traffic, carries COMMAND packets that are sent by CS to SNs and other nodes. In the presence of both forward and reverse traffics, this chapter investigates the performance of 2HCR protocol, and compares with 802.11b. Two situations are considered: situation one, symmetric traffic, when both traffic sources generate traffic at the same data rate, varying from 20 kbps to 800 kbps; situation two, asymmetric traffic, where DATA source generate traffic at various data rate (between 20 kbps to 800 kbps) and the COMMAND source generate traffic at 20 kbps.

As the COMMAND traffic is more important than data traffic, it is expected that COMMAND traffic should receive better treatment, in terms of packet delivery rate and packet loss ratio. Therefore, it is first examined if our proposed protocol, 2HCR, can still perform better than 802.11b in bi-directional scenario and meet priority support requirement. Simulation results in Section 5.2 show that 2HCR still performs better than 802.11b, but both protocols cannot meet the priority requirement. The simulation results show that both protocols deliver more or less the same packet delivery rate in symmetric setting but lower packet delivery rate for COMMAND traffic in asymmetric case.

In Section 5.3, 802.11e priority support mechanism is implemented to provide priority for COMMAND traffic. An 802.11e-like mechanism is incorporated to 2HCR protocol for COMMAND traffic. Simulation results show that such mechanism can provide priority support for symmetric setting but fail for symmetric case. When the COMMAND traffic rate is much lower than forward data traffic, COMMAND traffic still receives lower delivery rate. It may be due to hidden terminal problem.

To address the hidden terminal problem, RTS/CTS mechanism [18] is adopted in Section 5.4 for COMMAND traffic. In this section, it is proposed to implement RTS/CTS mechanism for COMMAND traffic while basic CSMA/CA mechanism is chosen for forward DATA traffic. Simulation results still show that higher delivery rate achieved for COMMAND traffic for symmetric setting and lower delivery rate for COMMAND traffic in asymmetric case.

To provide higher delivery rate for COMMAND traffic, even in asymmetric setting, we proposed to combine the principles in 802.11e and RTS/CTS in a new priority support scheme in Section 5.5. The new priority support scheme proposes implementation of RTS/CTS mechanism for COMMAND traffic and shorter IFS and smaller CW for RTS to access the medium. In other words, shorter IFS and smaller CW concept is adopted for COMMAND traffic to access the medium earlier than DATA traffic and RTS/CTS is implemented to minimize hidden terminal problem for COMMAND traffic. Simulation results show that this proposed simple priority support scheme can achieve higher delivery rate for COMMAND traffic, in both symmetric and asymmetric settings. The conclusion of this chapter is in Section 5.6.

5.2 PERFORMANCE OF 2HCR, 802.11b, AND MC CSMA IN BIDIRECTIONAL TRAFFIC

In this section, several simulations are conducted to examine the performance of 2HCR protocol in comparison with 802.11b, MC CSMA protocols in the presence of bidirectional traffic. The first simulation evaluates the performance of those three protocols in symmetric traffic setting. It will be investigated whether 2HCR protocol still outperforms the other two protocols as in unidirectional traffic scenario discussed in Chapter 3. Moreover, a further simulation is conducted to investigate the performance of 2HCR, in asymmetric setting. For comparison purpose, 802.11b is also evaluated.

To simplify traffic measurement on both directions, a simple chain topology shown in Figure 5-1 is used during the simulation where local head (LH) is the DATA traffic source and backbone node (BN) is the COMMAND traffic source respectively.

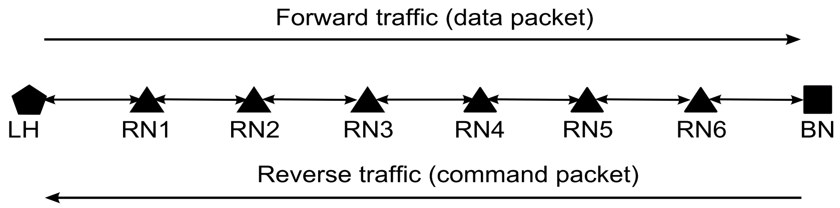

Figure 5-1 A chain network with 1-data source 1-command source 7-hop

For the first simulation, Figures 5-2 shows the throughput of both reverse and forward traffics. It can be seen that 2HCR still outperforms 802.11b and MC CSMA protocols. The maximum achievable throughput of 2HCR for both traffics is almost the same at 126 kbps, while the MC CSMA maximum achievable throughput is 118 kbps. On the other hand, the highest throughput for 802.11b is only 49 kbps. If the overall throughput is compared with unidirectional scenario, it can be noticed that bidirectional overall throughput is a bit lower than unidirectional. For example, the bidirectional overall highest throughput for 2HCR is 244 kbps, while the unidirectional highest throughput is 247 kbps. It may be due to more competition between two directions.

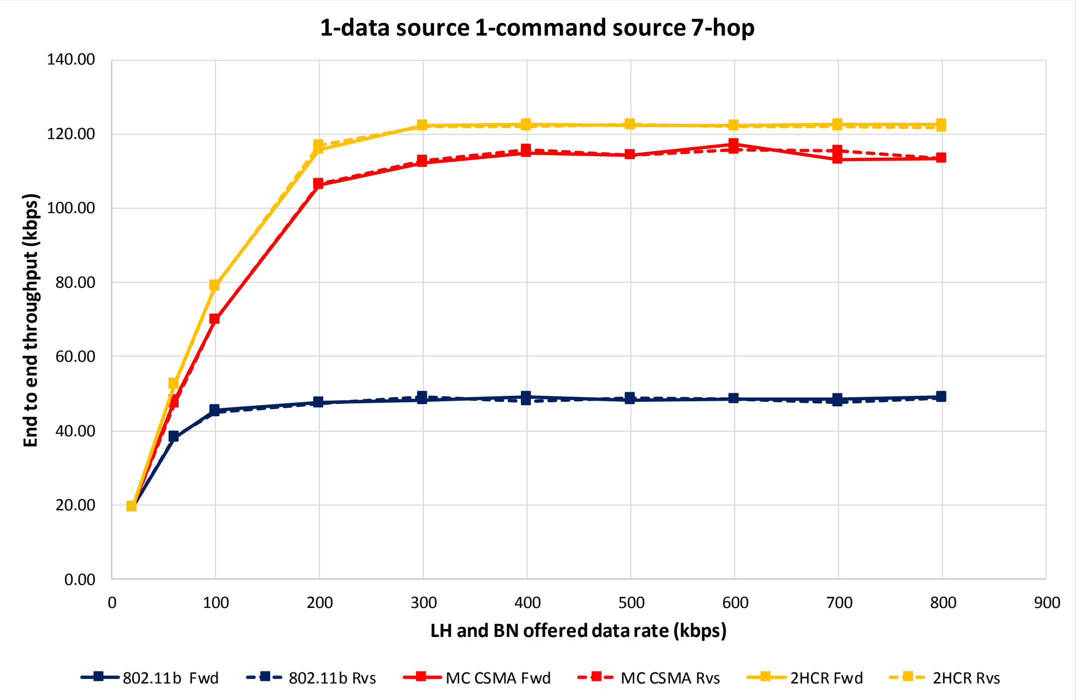

Figure 5-2 Throughput of 802.11b, MC CSMA, and 2HCR forward and reverse traffics

Furthermore, as shown in Figure 5-3, packet delivery rate of all protocols at the data rate of 20 bps are about 97 %. However, for data rate over 20 kbps, 2HCR achieves better packet delivery rate. The higher packet delivery rate derived by 2HCR shows that this protocol has better performance than 802.11b and MC CSMA in delivering packet to its destination. Moreover, packet loss rates of 2HCR, 802.11b and MC CSMA are shown in Figure 5-4. It shows that 2HCR achieves the lowest packet loss rate, compared to other protocols.

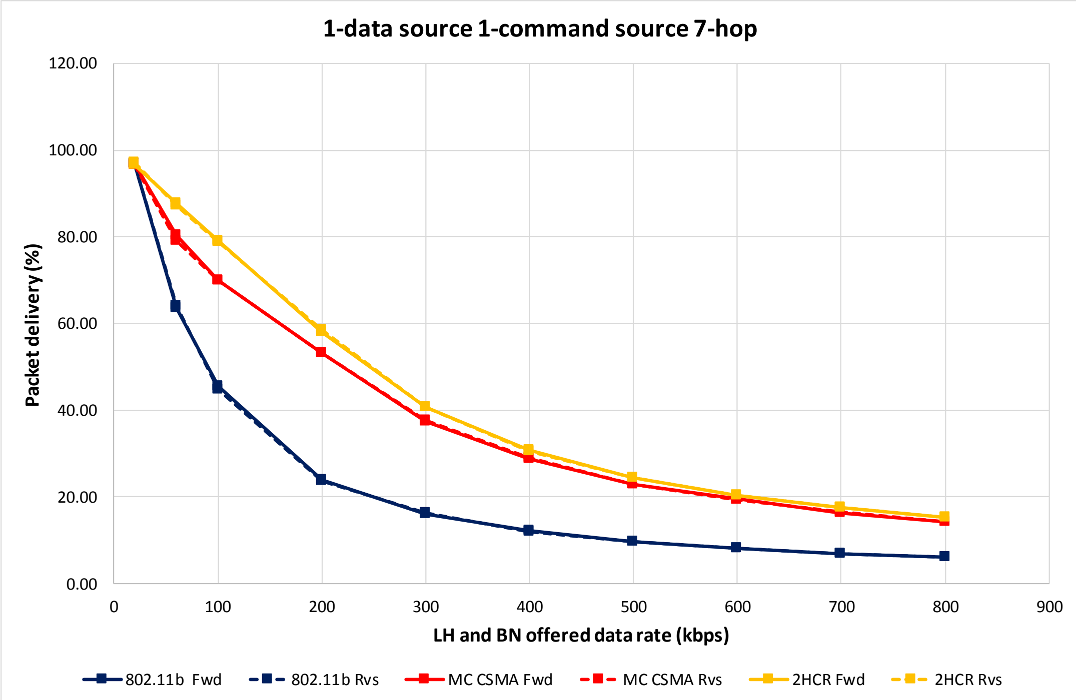

Figure 5-3 Packet delivery rate of 802.11b, MC CSMA, and 2HCR forward and reverse traffics

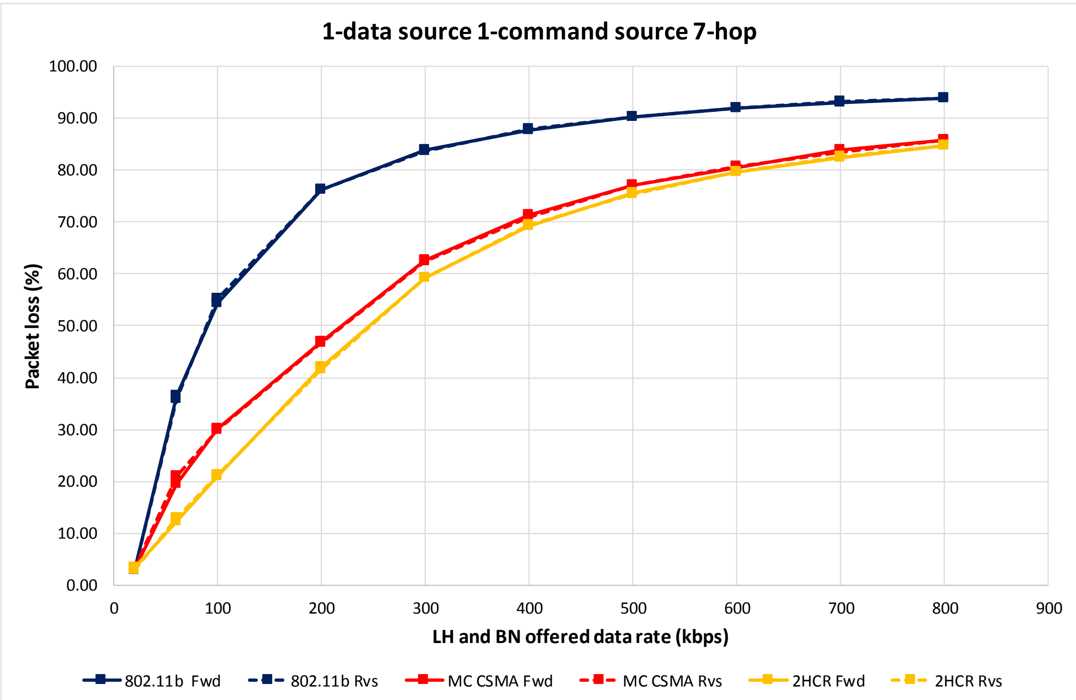

Figure 5-4 Packet loss rate of 802.11b, MC CSMA, and 2HCR forward and reverse traffics

The second simulation investigates the performance for asymmetric setting. The data rate for DATA traffic varies from 20 kbps to 800 kbps while the COMMAND traffic rate keeps at 20 kbps. For 802.11b protocol, the throughput of reverse and forward traffics is depicted in Figure 5-5. It is shown that the throughput of forward traffic increases along with the rise of LH data rate. The throughput then remains steady about 97 kbps as the network is saturated. In contrast, the throughput of reverse traffic is about 20 kbps for LH data rate of 20 kbps, then gradually decreases to achieve only 1 kbps at the LH data rate of 800 kbps. This indicates that forward traffic dominates network occupation and gives less opportunity for the reverse traffic in accessing the network.

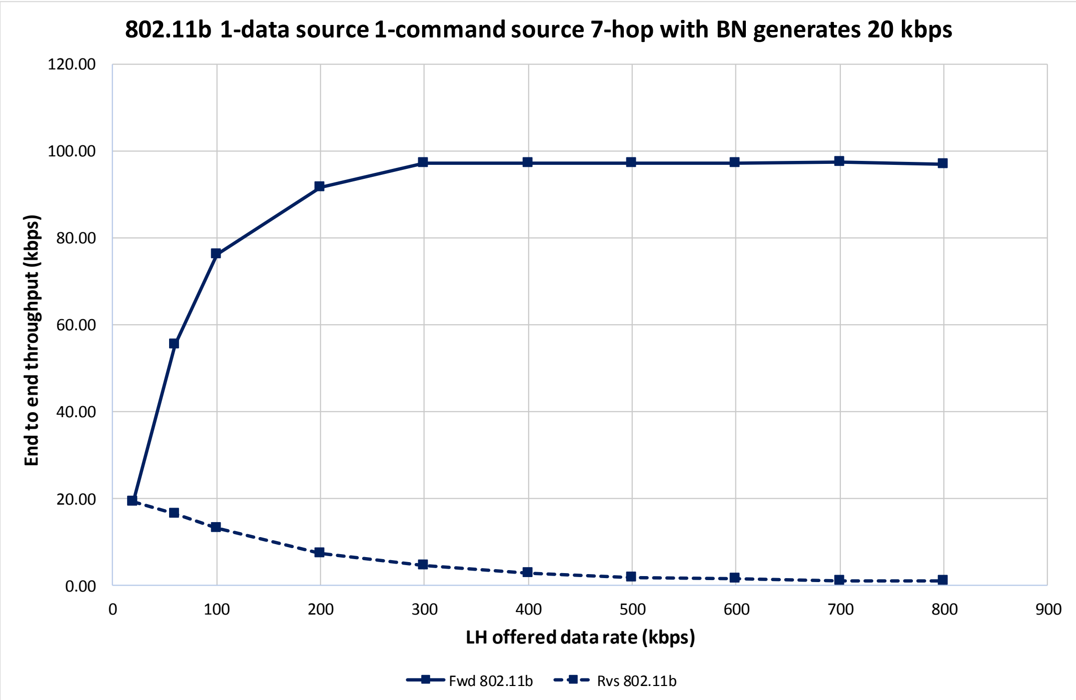

Figure 5-5 Throughput of 802.11b forward and reverse traffics, with BN generates 20 kbps

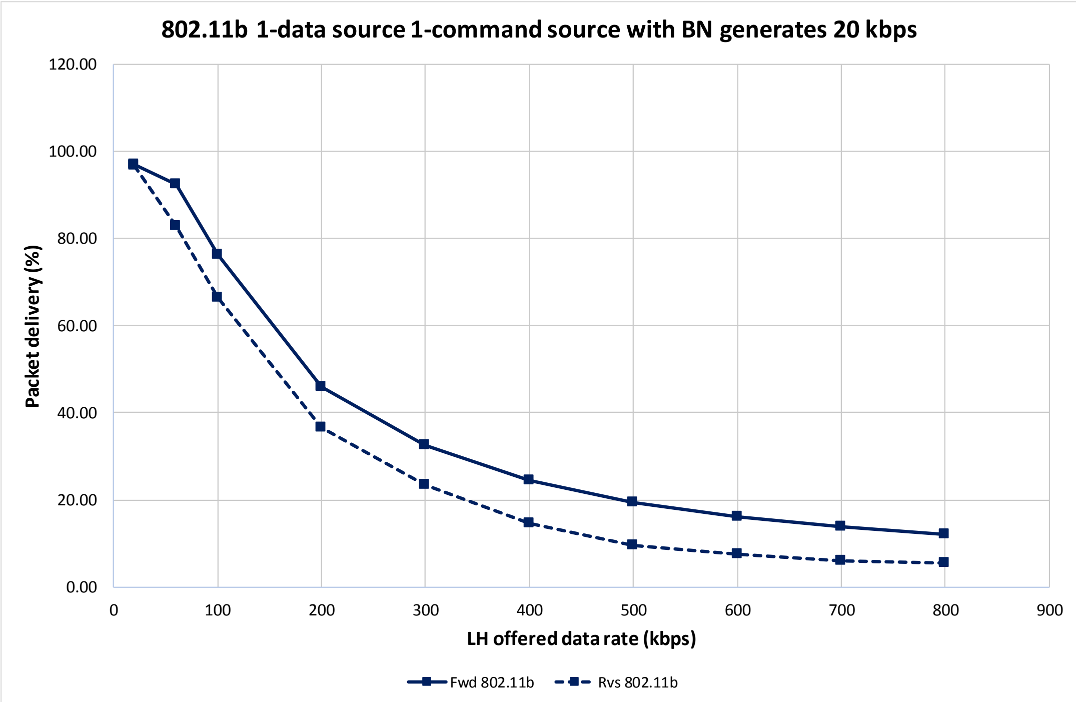

Figure 5-6 Packet delivery rate of 802.11b forward and reverse traffics, with BN generates 20 kbps

As forward packet dominates channel access, packet delivery rate of reverse traffic is lower than that of forward traffic as shown in Figure 5-6. The lowest packet delivery rate of reverse traffic reaches 5.42 % while the lowest packet delivery rate of forward traffic is 12.14 %. Both are obtained at LH data rate of 800 kbps. Packet delivery rate of both reverse and forward traffics is similar only at LH data rate of 20 kbps. At this point, packet delivery rate of both traffics is 97 %. As packet delivery rate of reverse traffic is lower than that of forward traffic, packet loss rate of reverse traffic is higher than the packet loss rate of forward traffic as shown in Figure 5-7. The highest packet loss rates of reverse and forward traffics are 94 % and 87 % respectively.

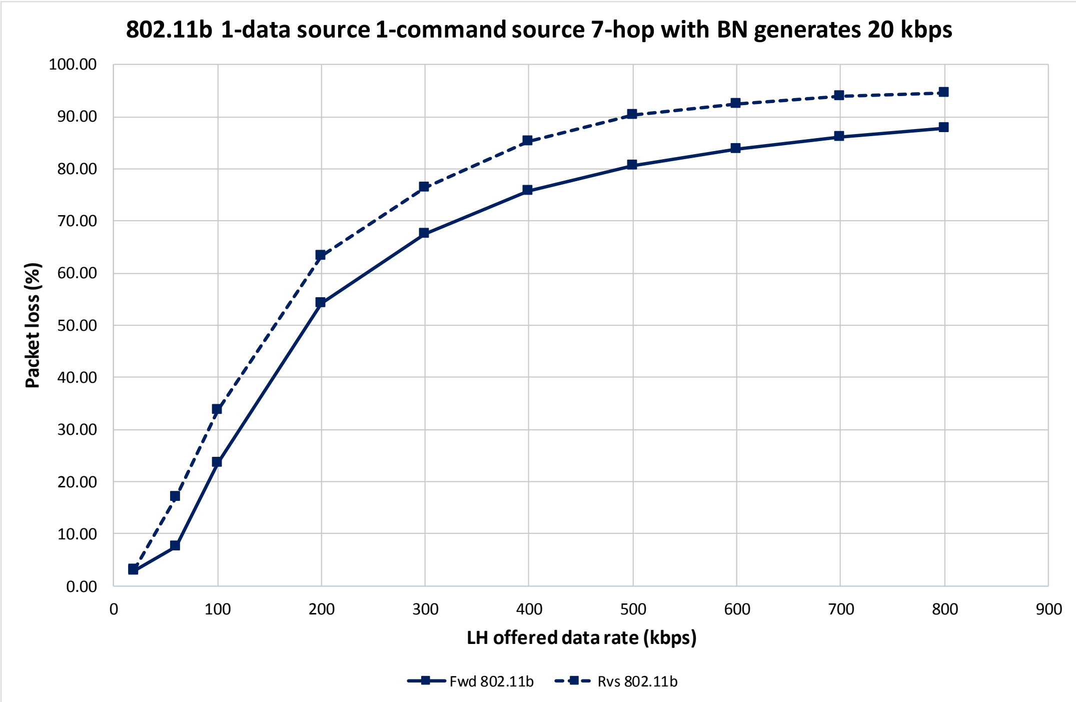

Figure 5-7 Packet loss rate of 802.11b forward and reverse traffics, with BN generates 20 kbps

We have also conducted simulation for 2HCR in asymmetric setting. The throughput of reverse and forward traffics is shown in Figure 5-8. It shows that the throughputs of forward traffic are 19.57 kbps at the LH data rate of 20 kbps. The throughput then increases along with the rise of LH data rate and saturates about 238 kbps. On the other hand, the throughput of reverse traffic is 19.41 kbps at LH data rate of 20 kbps, then decreases gradually to obtain only 2.56 kbps at LH data rate of 800 kbps.

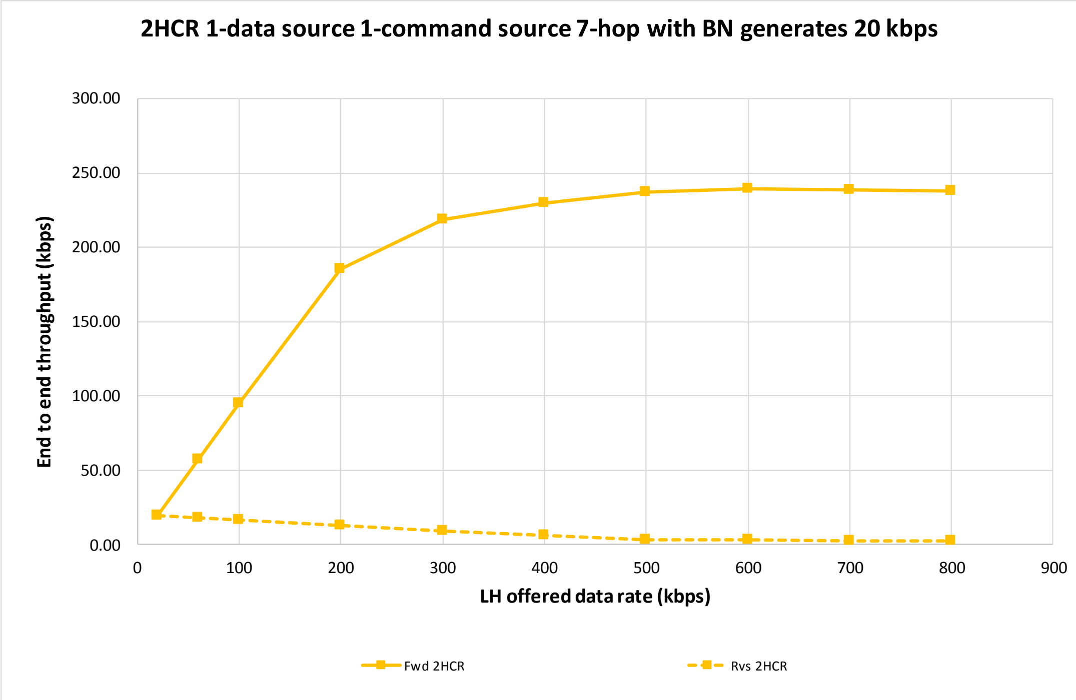

Figure 5-8 Throughput of 2HCR forward and reverse traffics, with BN generates 20 kbps

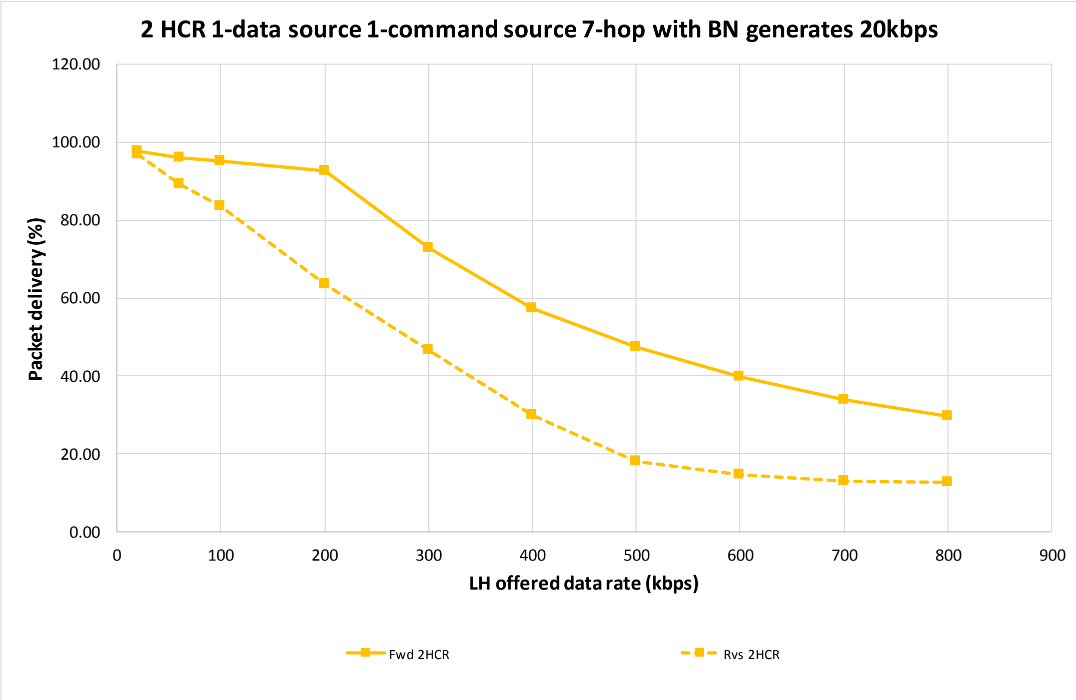

Figure 5-9 Packet delivery rate of 2HCR forward and reverse traffics, with BN generates 20 kbps

Similar with trend in 802.11b protocol, the domination of forward traffic in accessing the shared network has given less chance for reverse traffic to deliver packet to its destination. This situation impacts packet delivery rate of reverse traffic as shown in Figure 5-9. While packet delivery rate of reverse and forward traffics is similar at LH data rate of 20 kbps, i.e., about 97 %, the reverse traffic packet delivery rate is lower than the forward traffic packet delivery rate for higher LH data rate. The lowest packet delivery rate of reverse traffic achieves only 12.80 % whereas the lowest packet delivery rate of forward traffic can achieve 29.71 % when LH data rate is 800 kbps. Figure 5-10 shows the packet loss rate for 2HCR in asymmetric setting. It can be seen that reverse traffic has higher packet loss rate when LH data rate is higher than COMMAND generation rate.

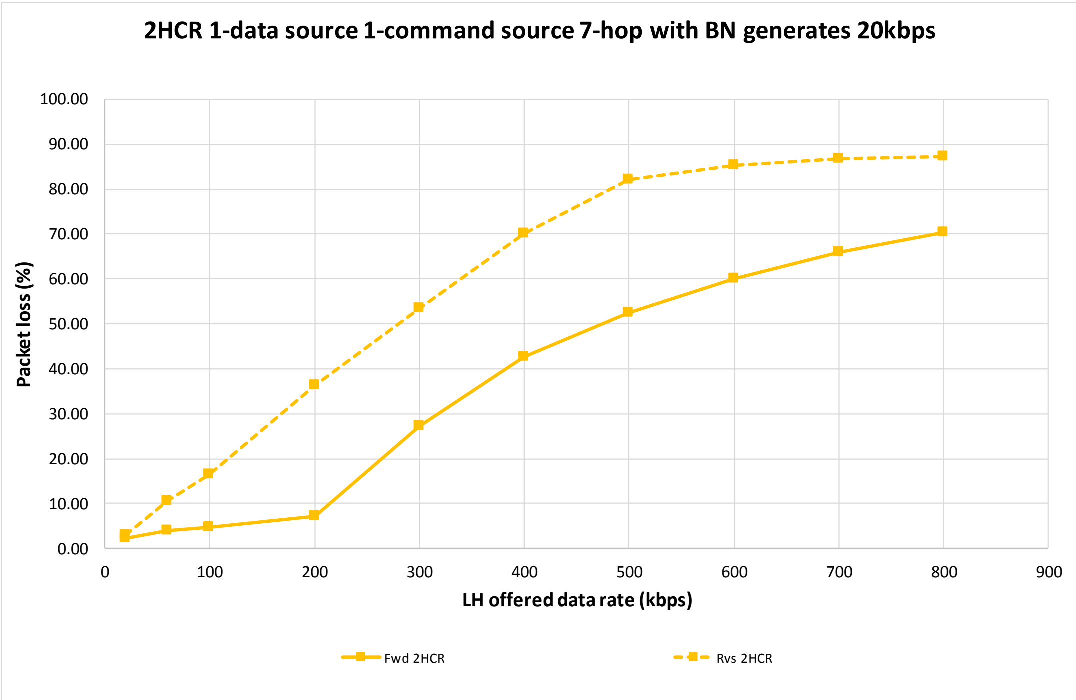

Figure 5-10 Packet loss rate of 2HCR forward and reverse traffics, with BN generates 20 kbps

For asymmetric setting where data rate of reverse traffic is lower than the data rate of forward traffic, it can be seen that packet delivery rate of reverse traffic is lower than that of forward traffic. Network utilization is dominated by forward traffic as it has much higher data rate. As the COMMAND traffic is considered more important than DATA traffic and should receive higher delivery rate, a priority support must be applied to COMMAND traffic in order to increase its packet delivery rate. One possibility is to implement 802.11e or similar mechanisms as discussed in the next section.

5.3 802.11e PROTOCOL TO PROVIDE PRIORITY SUPPORT IN BIDIRECTIONAL TRAFFIC

As mentioned in Section 2.6 of Chapter 2, 802.11e standard [39] is introduced as a complement for the previous 802.11 standard to handle quality of service (QoS) over wireless local area network (WLAN). Service differentiation is assigned to four types of packet to create packet priority described in Table 2-1 of Section 2.6. Referring to Table 2-1, voice packet has the highest priority whereas background packet has the lowest priority. Thus, voice packet has the shortest interframe space (IFS) and smallest contention window (CW) size compared with other packets. This allows voice packet to access the channel earlier than the other packets during a channel contention. On the other hand, the background packet has the longest IFS and biggest CW size, which makes it to have less opportunity to access channel, compared with other packets. This service differentiation mechanism will be implemented in this section to bidirectional network in order to enhance the packet delivery rate of reverse traffic.

As reverse traffic is demanded to have a higher priority than the forward traffic, IFS and CW of voice packet in 802.11e are assigned to reverse traffic. Meanwhile, IFS and CW of background packet are assigned to forward traffic. For evaluation purpose, this setting is applied to two situations addressed in Chapter 5.2, where reverse and forward traffics have the same data rate in symmetric situation, while reverse traffic data rate is lower than forward traffic data rate in asymmetric setting. The size of time slot is 20 micro seconds.

For symmetric situation with 802.11b protocol, Figure 5-11 shows the throughput of 802.11b forward and reverse traffics before and after 802.11e priority protocol is applied. The use of 802.11e can slightly increase the reverse traffic throughput. On the other hand, the throughput of forward traffic is slightly decreased. Therefore, the rise of reverse traffic throughput consequently reduces the throughput of forward traffic with a similar proportion. Furthermore, the reverse traffic throughput improvement leads to the rise of reverse packet delivery rate. As depicted in Figure 5-12, reverse traffic packet delivery rate increases a little bit. Meanwhile, packet delivery rate of forward traffic is slightly decreased. Similar with the throughput, the increase of reverse traffic packet delivery rate proportionally reduces the packet delivery rate of forward traffic. Figure 3-13 shows the packet loss ratio for both forward and reverse traffics. It can be seen that COMMAND traffic has a slightly lower packet loss ratio than that of DATA traffic, when higher priority is assigned to it.

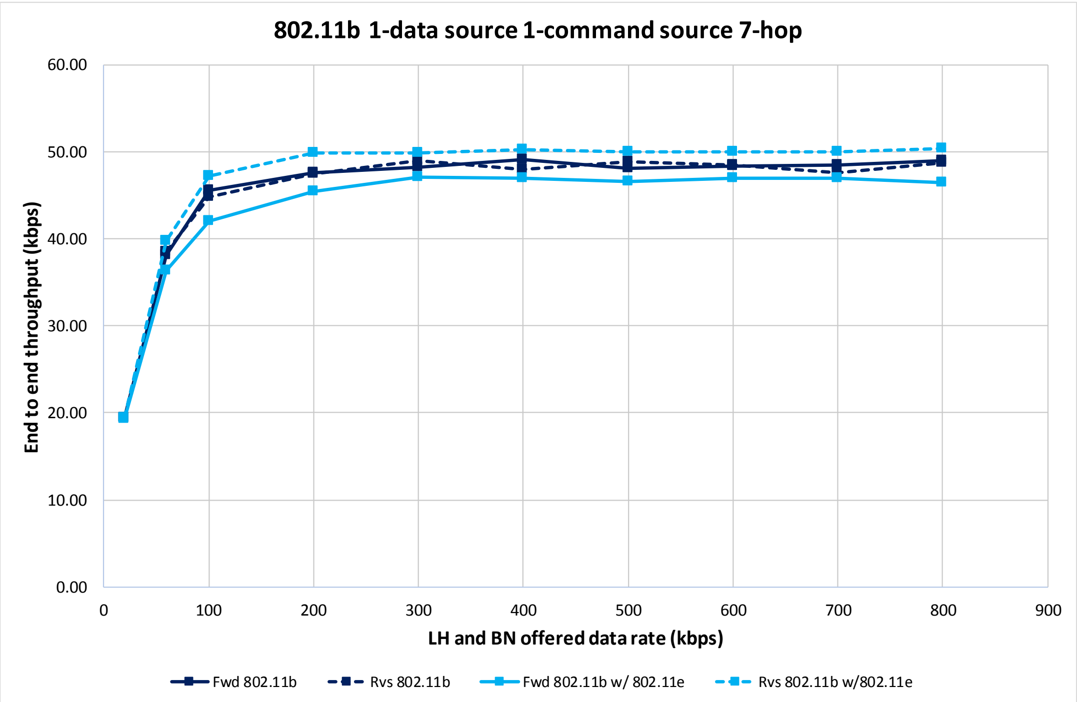

Figure 5-11 Throughput of 802.11b forward and reverse traffics implementing 802.11e priority

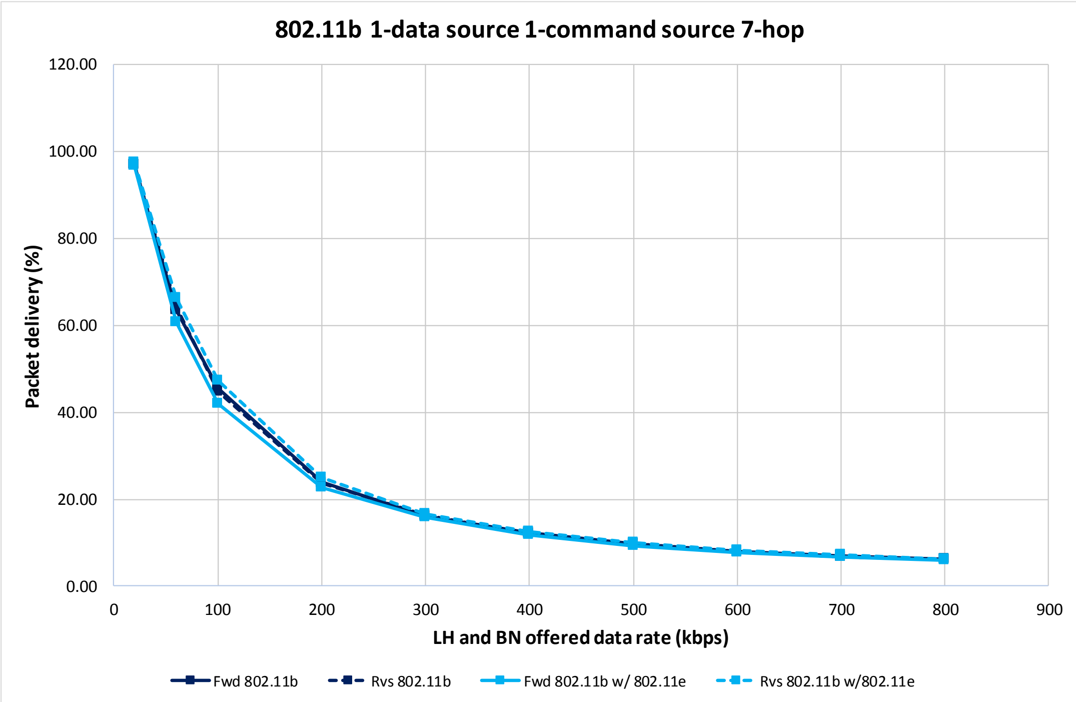

Figure 5-12 Packet delivery rate of 802.11b forward and reverse traffics implementing 802.11e priority

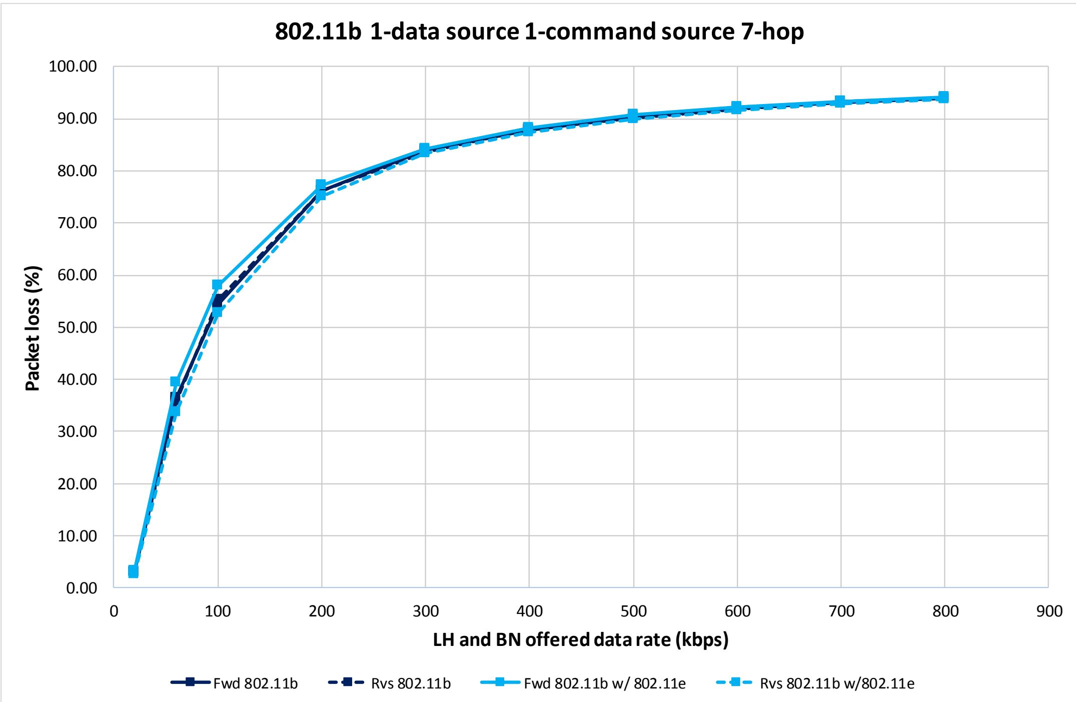

Figure 5-13 Packet loss rate of 802.11b forward and reverse traffics implementing 802.11e priority

For asymmetric situation where data rate of reverse traffic is 20 kbps while the forward traffic data rate varies from 20 kbps to 800 kbps, the throughput of reverse and forward traffics with 802.11b protocol is shown in Figure 5-14. With the use of 802.11e priority support, the throughput of reverse traffic can slightly increase, while the throughput of forward traffic slightly decreases.

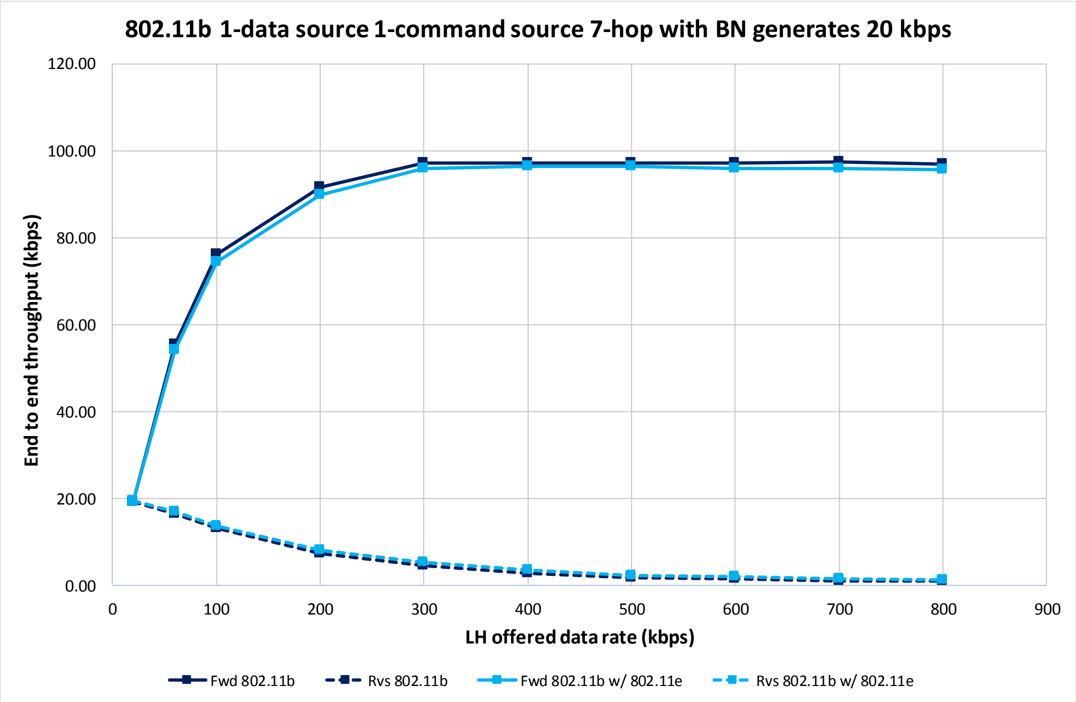

Figure 5-14 Throughput of 802.11b forward and reverse traffics implementing 802.11e priority, with BN generates 20 kbps

The improvement on reverse traffic throughput causes the improvement of its packet delivery rate as depicted in Figure 5-15. However, this enhancement could not bring the reverse traffic packet delivery rate above the packet delivery rate of forward traffic. The reverse traffic packet delivery rate still below the forward traffic packet delivery rate although 802.11e protocol reduces the throughput of forward traffic. It can be seen that the use of shorter IFS and smaller CW in bidirectional traffic with asymmetric situation could not provide enough priority support for reverse traffic to access the channel. A possible reason is because the overwhelm forward traffic packet may still hinder reverse traffic packet to access the channel, even though the reverse traffic has a shorter time to access the channel than the forward traffic. Hence, using only shorter IFS and CW may not be sufficient, and therefore it requires another mechanism to better improve reverse traffic packet delivery rate. Furthermore, as packet delivery rate of reverse traffic increases, its packet loss rate reduces as shown in Figure 5-16. This packet loss rate is above the packet loss rate of forward traffic.

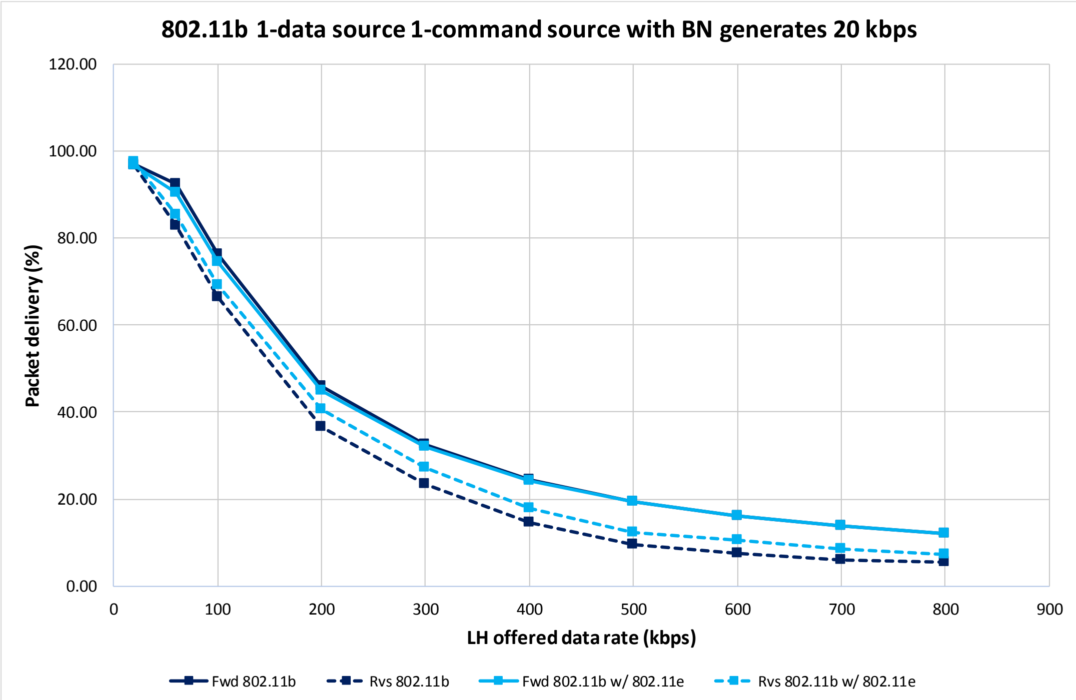

Figure 5-15 Packet delivery rate of 802.11b forward and reverse traffics implementing 802.11e priority, with BN generates 20 kbps

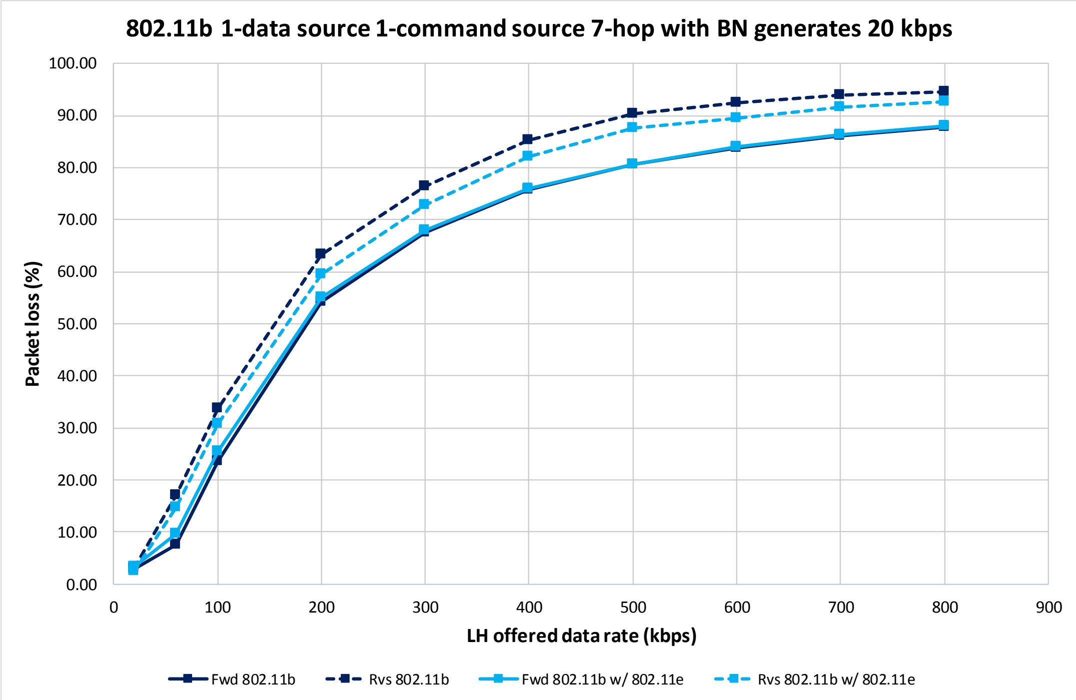

Figure 5-16 Packet loss rate of 802.11b forward and reverse traffics implementing 802.11e priority, with BN generates 20 kbps

Meanwhile, throughput of reverse and forward traffics for symmetric situation with 2HCR is shown in Figure 5-17. The reverse traffic throughput is improved a little bit, while the throughput of forward traffic slightly decreases. As like in the symmetric situation with 802.11b protocols, the increase of reverse traffic throughput is proportionally similar with the amount of forward traffic throughput degradation. As a result of reverse traffic throughput improvement, its packet delivery rate slightly increases as shown in Figure 5-18. On the other hand, the forward traffic packet delivery rate declines as its throughput is decreased. Furthermore, the packet loss rate of reverse traffic decreases slightly whereas the packet loss rate of forward traffic increases a little bit, as shown in Figure 5-19.

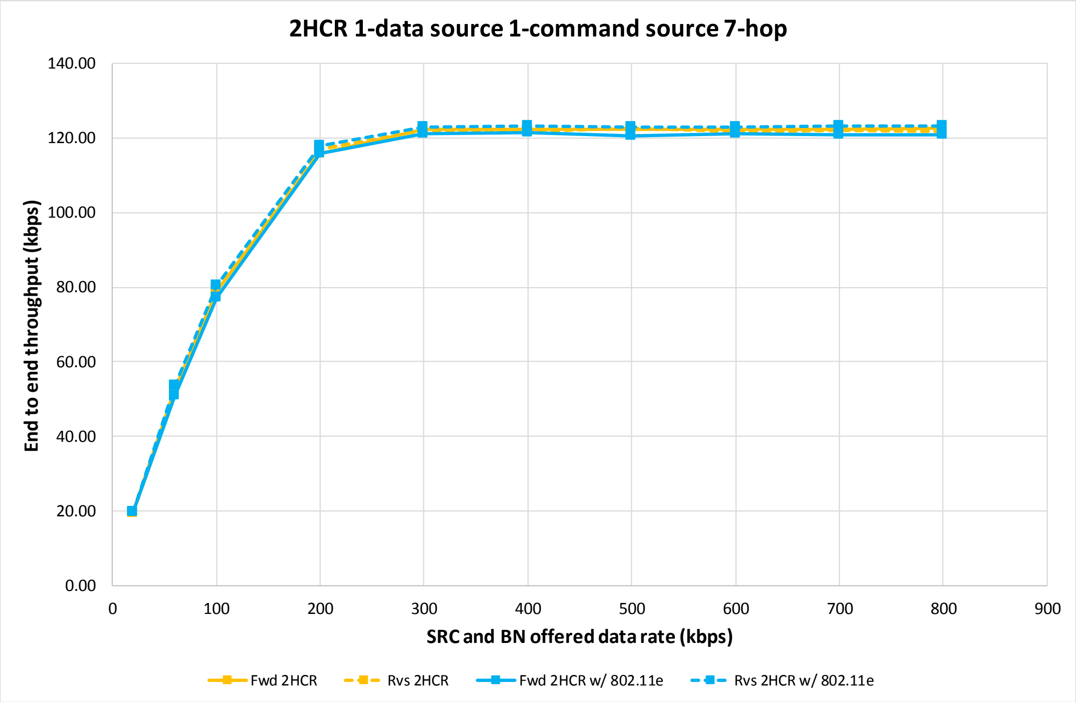

Figure 5-17 Throughput of 2HCR forward and reverse traffics implementing 802.11e priority

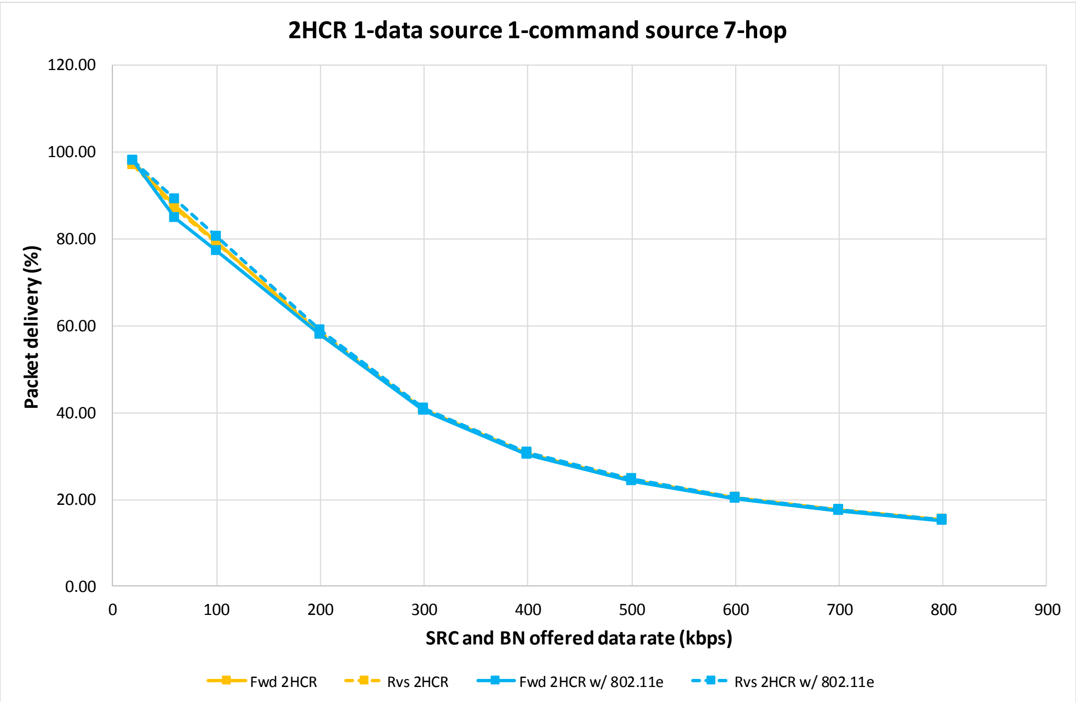

Figure 5-18 Packet delivery rate of 2HCR forward and reverse traffics implementing 802.11e priority

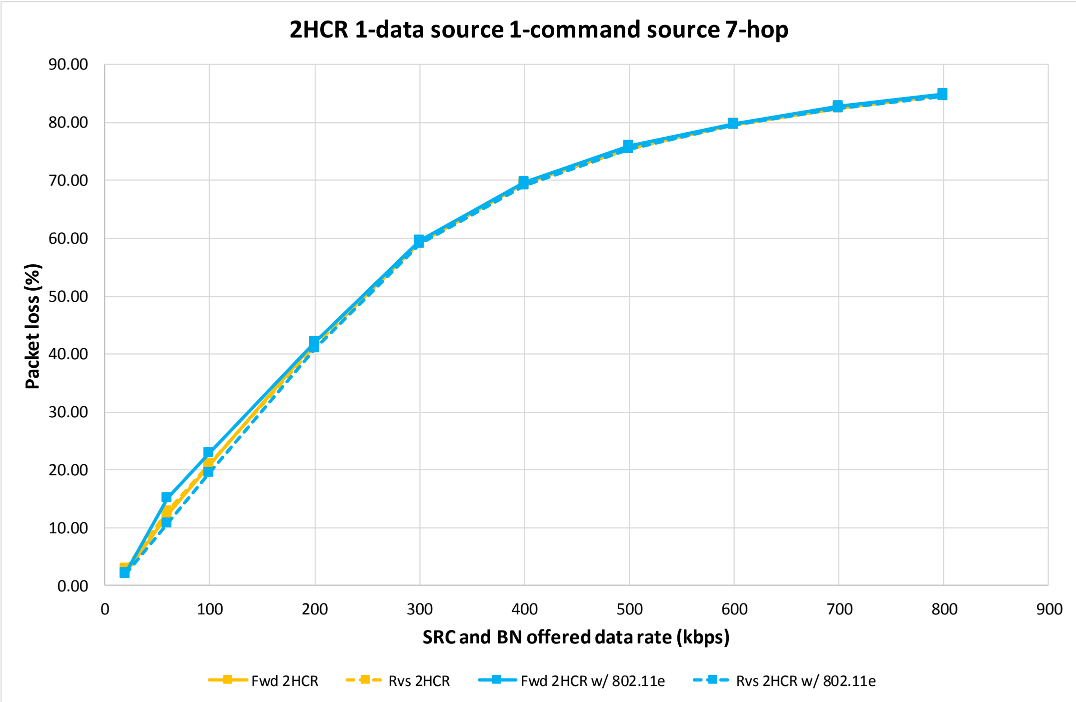

Figure 5-19 Packet loss rate of 2HCR forward and reverse traffics implementing 802.11e priority

For asymmetric situation with 2HCR, the throughput of reverse and forward traffics is depicted in Figure 5-20. When 802.1e priority support is implemented, reverse traffic throughput is improved while forward traffic throughput is decreased. Figure 5-21 shows the packet delivery ratio for both forward and reverse traffics. It can be seen that reverse traffic delivery ratio is improved significantly while forward traffic delivery ratio is decreased slightly. Unfortunately, with such a significant improvement, reverse traffic packet delivery rate is still lower than forward traffic packet delivery rate. As with 802.11b protocol, the heavy forward traffic may hinder reverse traffic in accessing the channel. Figure 5-22 shows the packet loss performance. It can be seen that reverse traffic packet loss is improved while forward traffic packet loss is increased, though reverse traffic still has higher packet loss ratio, compared to forward traffic.

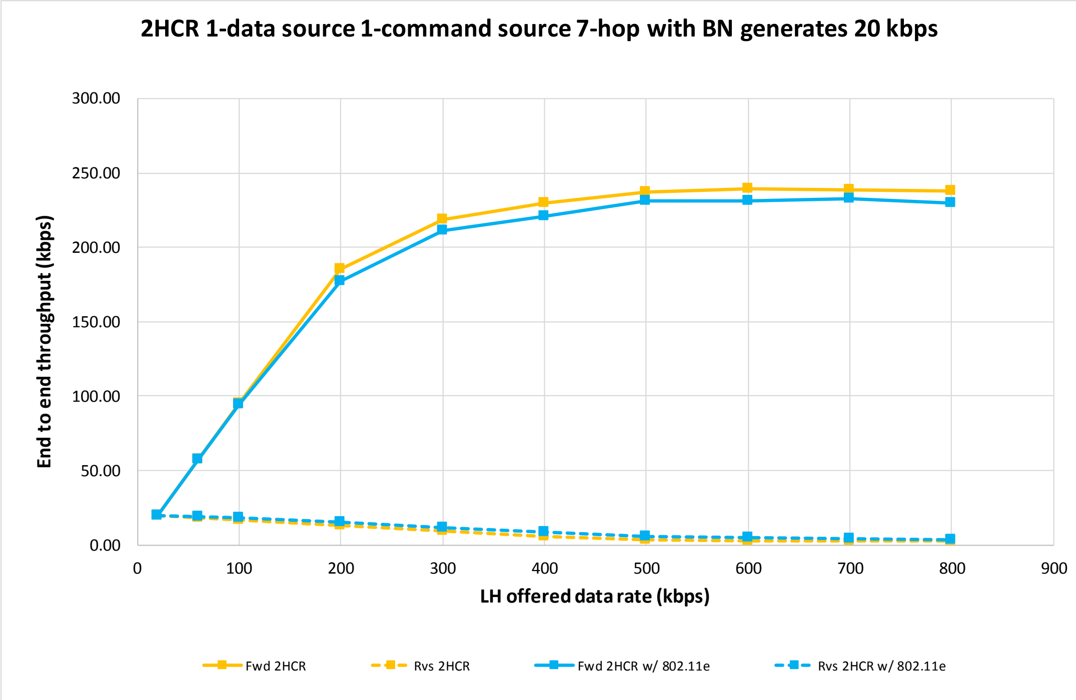

Figure 5-20 Throughput of 2HCR forward and reverse traffics implementing 802.11e priority, with BN generates 20 kbps

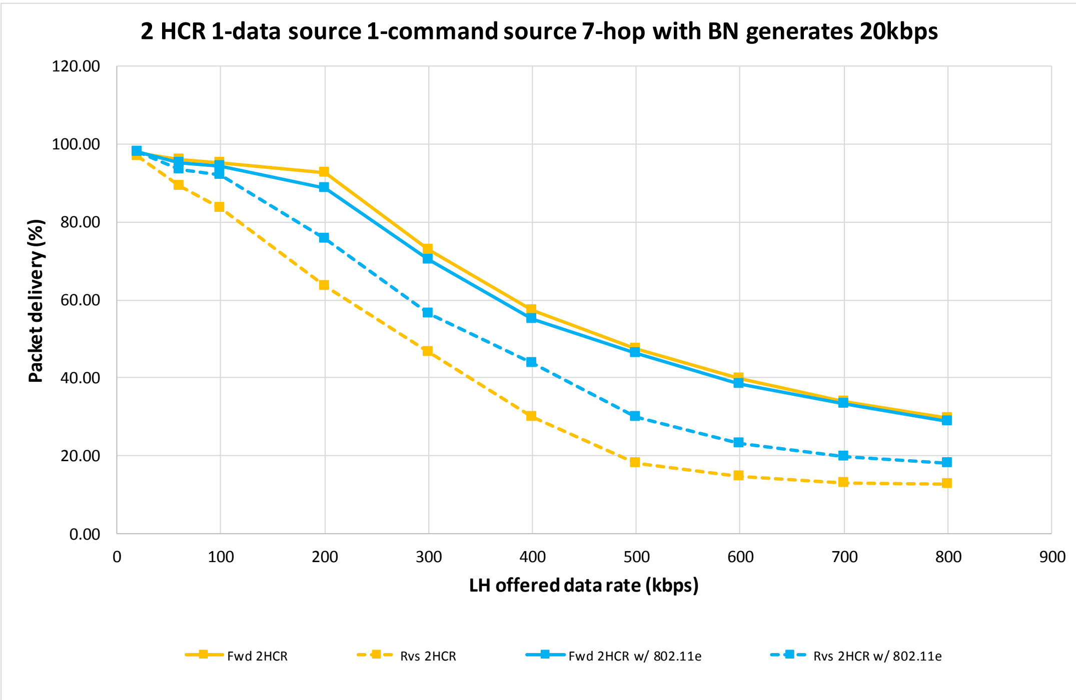

Figure 5-21 Packet delivery rate of 2HCR forward and reverse traffics implementing 802.11e priority, with BN generates 20 kbps

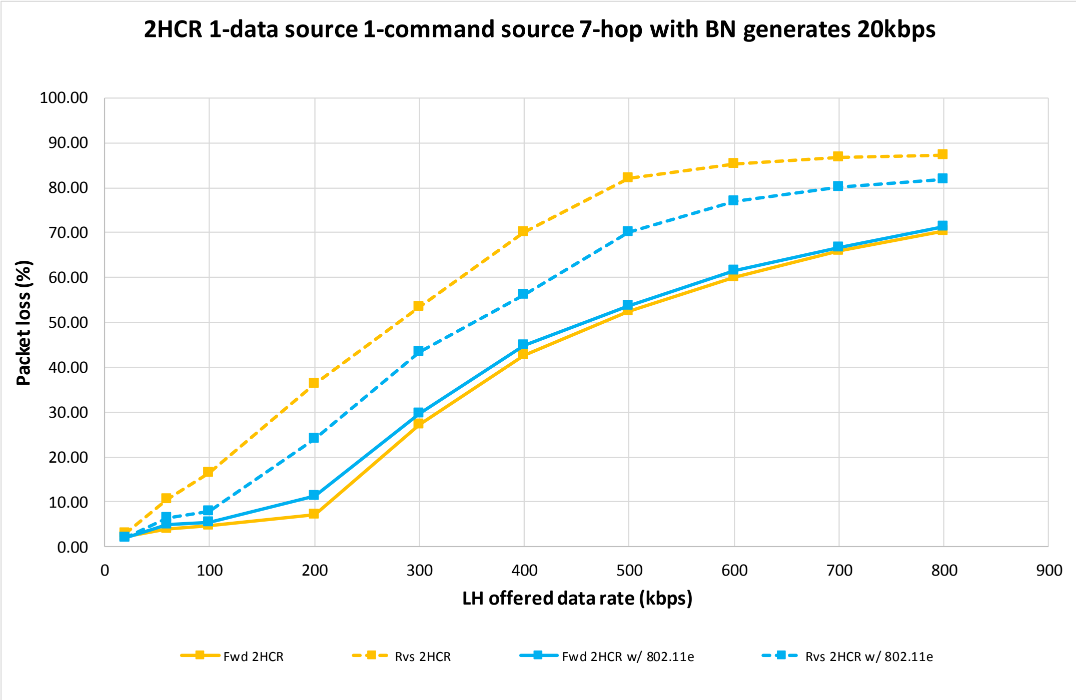

Figure 5-22 Packet loss rate of 2HCR forward and reverse traffics implementing 802.11e priority, with BN generates 20 kbps

The simulation results show that utilization of 802.11e for priority support could increase the chance of reverse traffic in accessing the channel resource when competing with forward traffic. However, for the asymmetric situation, the support may not be enough for reverse traffic to have higher packet delivery ratio than forward traffic. Therefore, we need to look at other options. In the next section, we consider implementing RTS/CTS mechanism to improve reverse traffic packet delivery ratio.

5.4 RTS/CTS PROTOCOL TO PROVIDE PRIORITY SUPPORT IN BIDIRECTIONAL TRAFFIC

It is shown in Section 5.3 that 802.11e mechanism cannot provide higher packet delivery rate for COMMAND traffic in asymmetric setting. It may be because that though shorter IFS and smaller CW give priority for COMMAND traffic to access the channel, it cannot protect COMMAND traffic from hidden terminal collision, which becomes more severe when forward DATA traffic increases. Therefore, to provide another strategy to improve packet delivery of reverse traffic significantly, it is first investigated the possible cause why reverse traffic packet may not be delivered properly. This is discussed in Section 5.4.1. Then, Section 5.4.2 addresses priority support based on RTS/CTS protocol. The effectiveness of the scheme is evaluated in Section 5.4.3. Hereafter, in Section 5.4.4 a modification is given to the scheme to achieve a better priority treatment.

5.3.1 Collision due to Hidden Node Problem in Bidirectional Traffic

Consider a part of multihop network illustrated in Figure 5-23. In this network, forward traffic flows from RN1 to RN3 via RN2. On the other hand, reverse traffic flows from RN3 to RN1 via RN2. As RN1 is a hidden node of RN3 and vice versa, their transmission may collide to each other at RN2 as shown in Figure 5-23. Although 2HCR protocol has a mechanism to prevent the effect of hidden node problem, it is proposed to reduce in-flow hidden collision and may not solve the hidden collision between flows. Therefore, hidden terminal collision between reverse and forward traffics may still occur, particularly if the forward traffic is heavier than the reverse traffic. Heavier the forward traffic, shorter time can be used by reverse traffic to achieve a successful packet delivery. Consequently, the reverse traffic packet delivery rate may be lower than the forward traffic packet delivery rate. To solve this problem, possibility is to supress the transmission of forward packet when reverse traffic is transmitting and RTC/CTS can be used for this purpose.

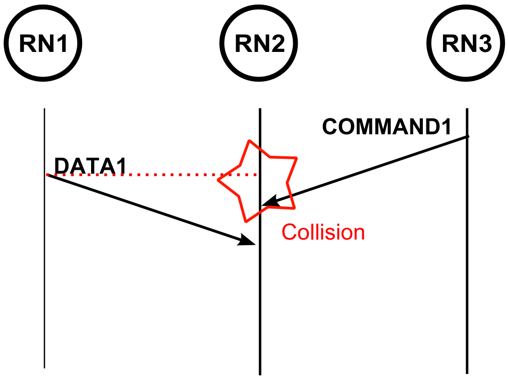

Figure 5-23 Packet collision caused by hidden node

5.3.2 RTS/CTS Based Priority Support

To supress forward traffic during COMMAND packet delivery, RTS/CTS is applied for reverse traffic as shown in Figure 5-24. RTS/CTS is exchanged prior to the COMMAND packet transmission. If node RN3 intends to send COMMAND packet to RN2, it first sends an RTS packet to RN2. While RTS packet is received by RN2, it is also overheard by to postpone its transmission during packet delivery from RN3 to RN2. Upon receiving RTS, RN2 responses the request by sending a CTS packet to RN3, deferring any transmission, and preparing itself to receive the COMMAND packet. Once RN3 received CTS packet, it sends COMMAND packet to RN2. Meanwhile, CTS packet is overheard by RN1. This gives information to RN1 to postpone its transmission until the COMMAND packet has been exchanged.

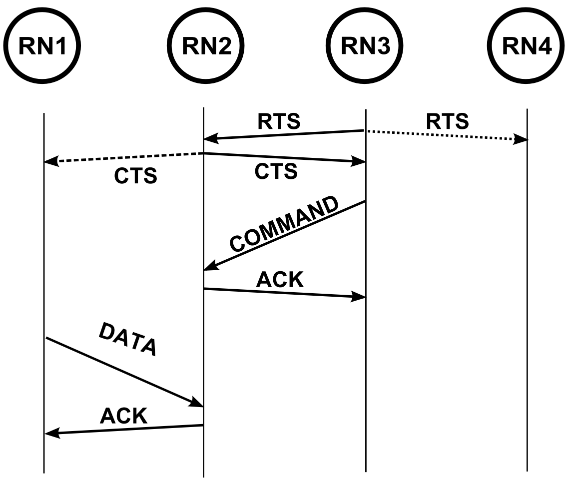

Figure 5-24 Providing a priority for reverse traffic by using RTS/CTS messages

The time line of RTS/CTS exchange prior to COMMAND packet transmission is shown in Figure 5-25. There are two interframe spaces (IFS) utilized during packet exchange. A distributed coordination function interframe space (DIFS) is used by RN3 prior to RTS transmission after it sensed that the channel is idle. On the other hand, a short interframe space (SIFS) is utilized by RN2 and RN3 prior to the transmission of either CTS, COMMAND, or ACK packet. There are also three holding transmission times undertaken by nodes. T_{h1} is run by RN4 upon receiving RTS. In 802.11 standard [18], it is known as RTS network allocation vector (RTS NAV). T_{h2}, on the other hand is undertaken by RN2 to prepare COMMAND packet reception. Meanwhile, T_{h3} is run by RN1 once it overheard CTS packet. In 802.11 protocol [18], it is known as CTS NAV.

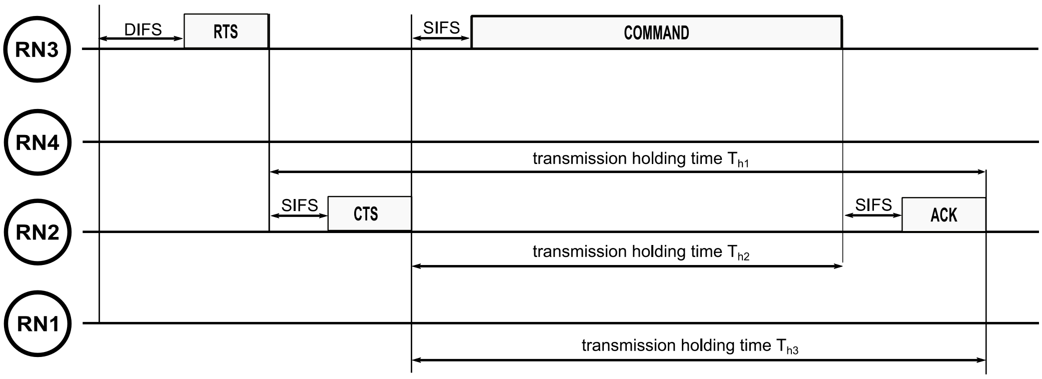

Figure 5-25 Packet exchange time line of priority support using RTS/CTS

Consider applying the above mechanism in multihop network with asymmetric situation, where the data rate of reverse traffic is significantly lower than the data rate of forward traffic. Each time a COMMAND packet is forwarded from a RN to another RN, the RTS/CTS transmission will prevent DATA packet transmission coming from the opposite direction. If this mechanism works properly along the entire network, the COMMAND packet can reach its destination, while some of DATA packet transmissions are postponed. Therefore, higher COMMAND packet delivery rate can be achieved. To evaluate the effectiveness RTS/CTS for priority support, simulations are conducted, and the results are discussed in the next subsection.

5.3.3 Performance Evaluation of RTS/CTS as Priority Support

This subsection evaluates the performance of RTS/CTS protocol in providing priority support for reverse traffic. Two setting discussed in Section 5.2 and 5.3 are considered for 802.11b and 2HCR protocols. For the symmetric setting with 802.11b protocol, the throughput of reverse and forward traffics is shown in Figure 5-26. By implementing RTS/CTS for supporting reverse traffic priority, the throughput of reverse traffic increases whilst the throughput of forward traffic decreases. The rise of reverse traffic throughput is proportional to the degradation of the forward traffic throughput. Furthermore, as the throughput of reverse traffic increases, its packet delivery rate also improves, as shown in Figure 5-2, and packet loss of reverse traffic decreases, as shown in Figure 5-28. In contrast, since the throughput of forward traffic declines, its packet delivery rate also decreases. This makes packet loss rate of forward traffic increases

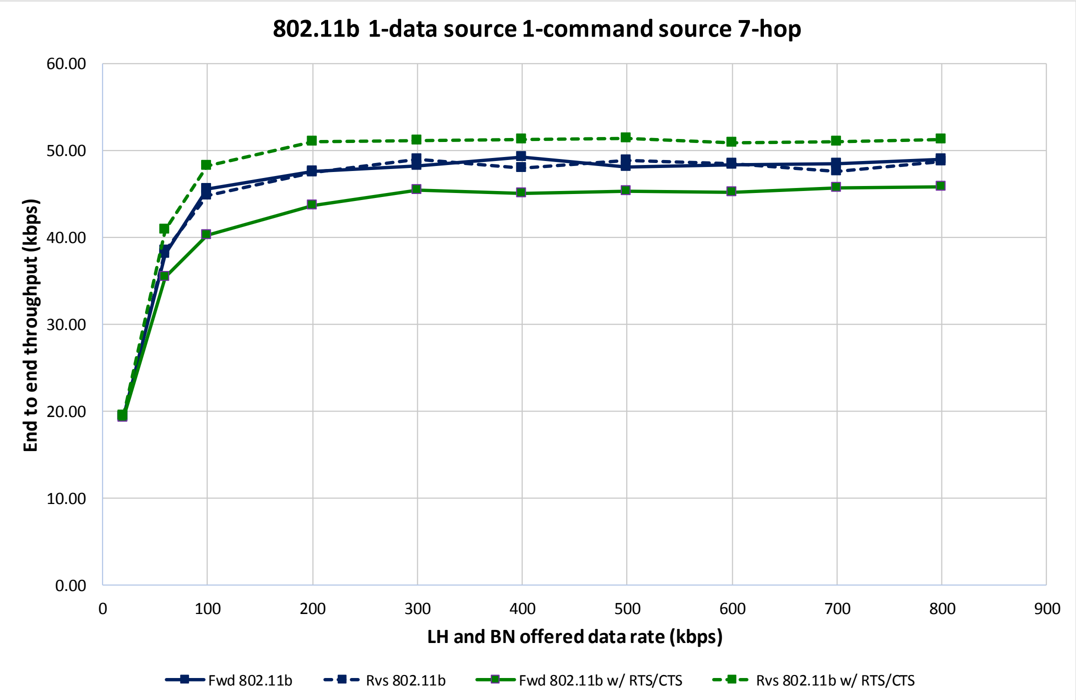

Figure 5-26 Throughput of 802.11b forward and reverse traffics implementing RTS/CTS for priority support

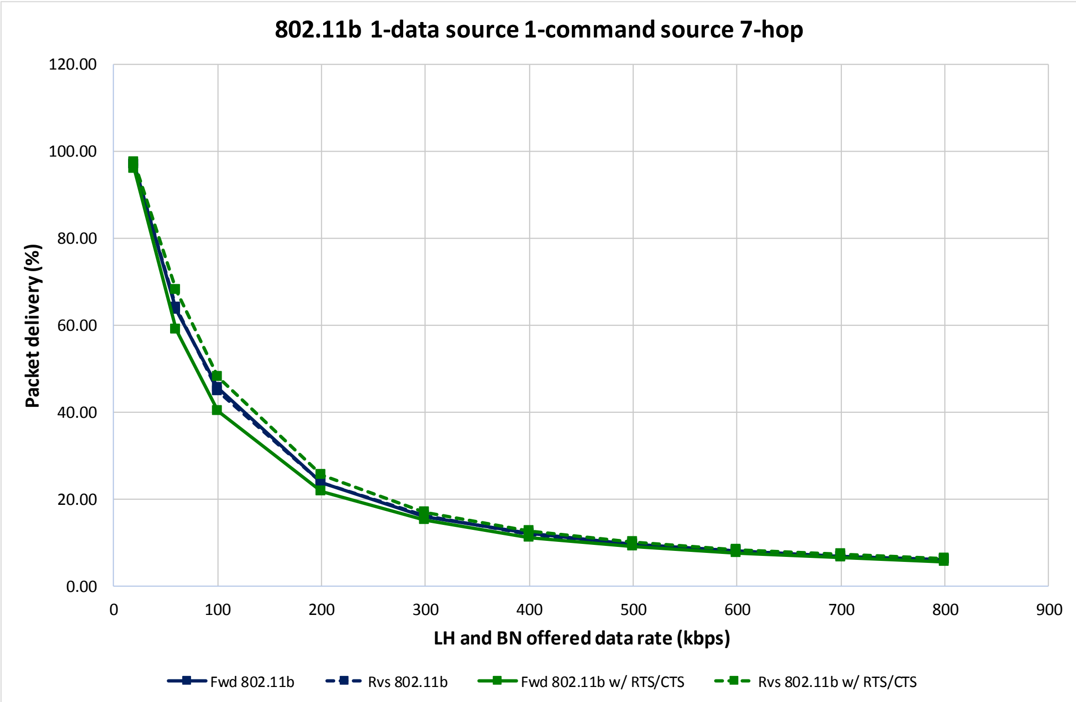

Figure 5-27 Packet delivery rate of 802.11b forward and reverse traffics implementing RTS/CTS for priority support

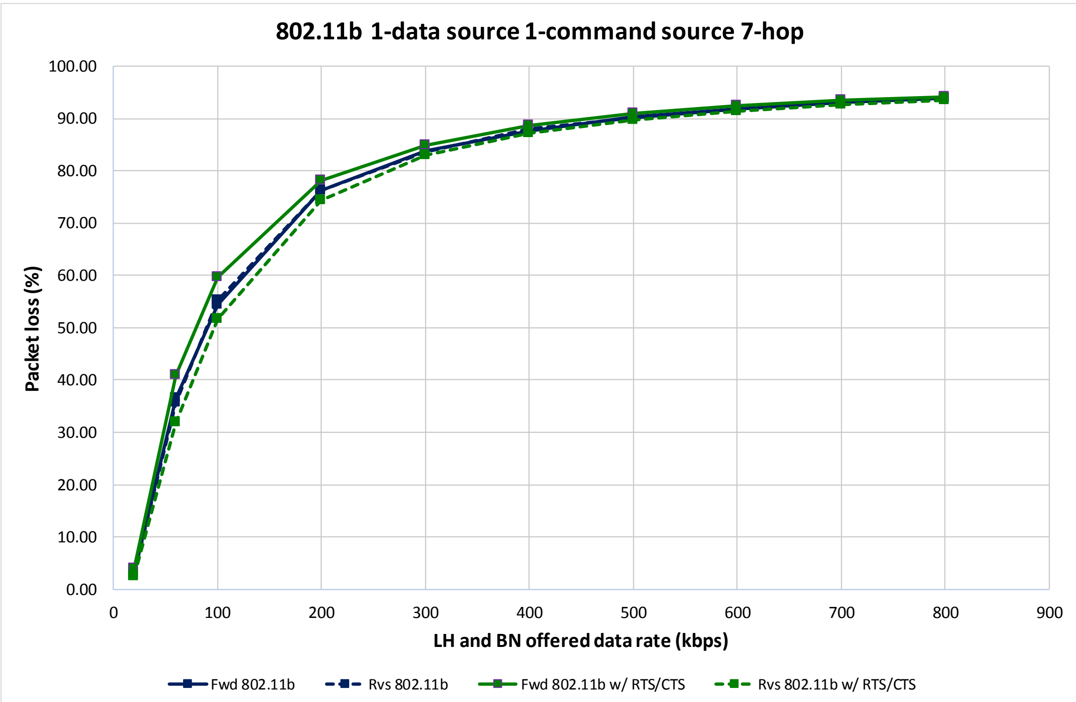

Figure 5-28 Packet loss rate of 802.11b forward and reverse traffics implementing RTS/CTS for priority support

For asymmetric situation with 802.11b protocol, the throughput of reverse and forward traffics is shown in Figure 5-29. It can be seen that reverse traffic throughput increases while forward traffic throughput decreases. The improvement of reverse traffic throughput gives a significant rise on its packet delivery rate, as shown in Figure 5-30. However, its packet delivery rate is still lower than the packet delivery rate of forward traffic. Nonetheless, the reverse traffic packet loss rate declines significantly as shown in Figure 5-31. On the other hand, throughput degradation of forward traffic causes only a slight decrease on its packet loss rate. As a result, its packet loss rate declines a little only.

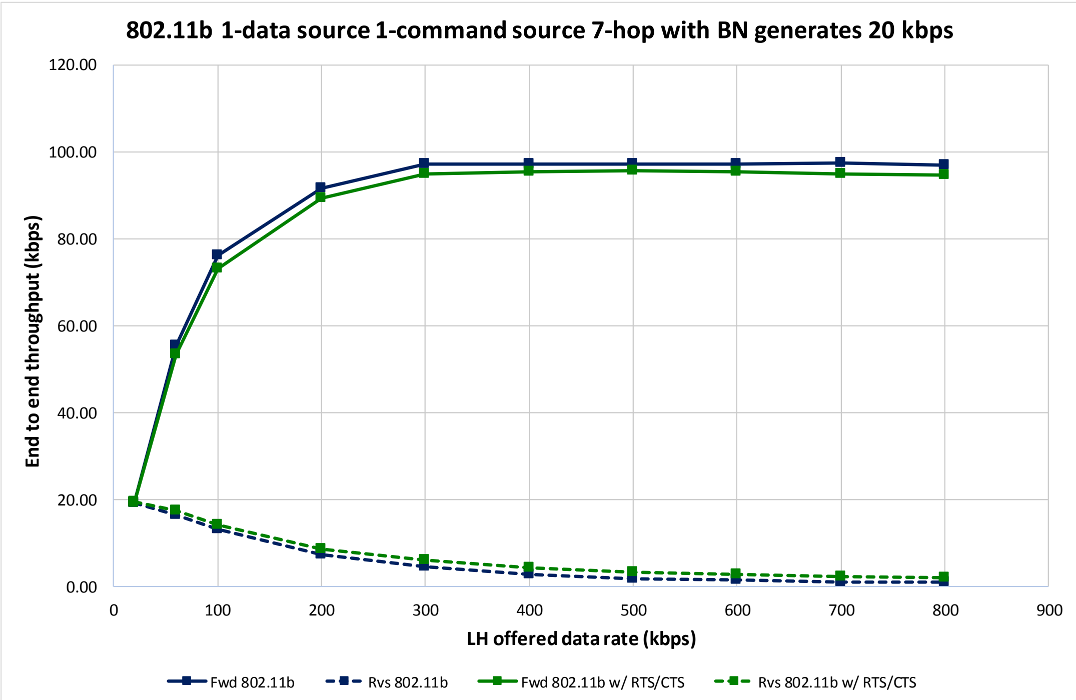

Figure 5-29 Throughput of 802.11b forward and reverse traffics implementing RTS/CTS for priority support, with BN generates 20 kbps

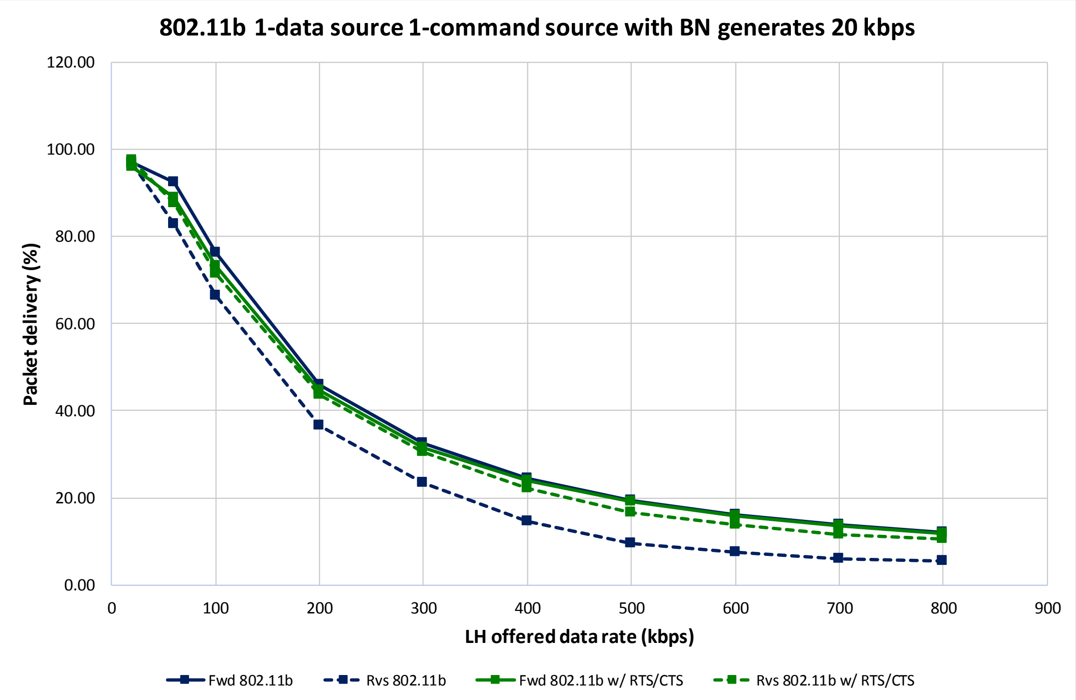

Figure 5-30 Packet delivery rate of 802.11b forward and reverse traffics implementing RTS/CTS for priority support, with BN generates 20 kbps

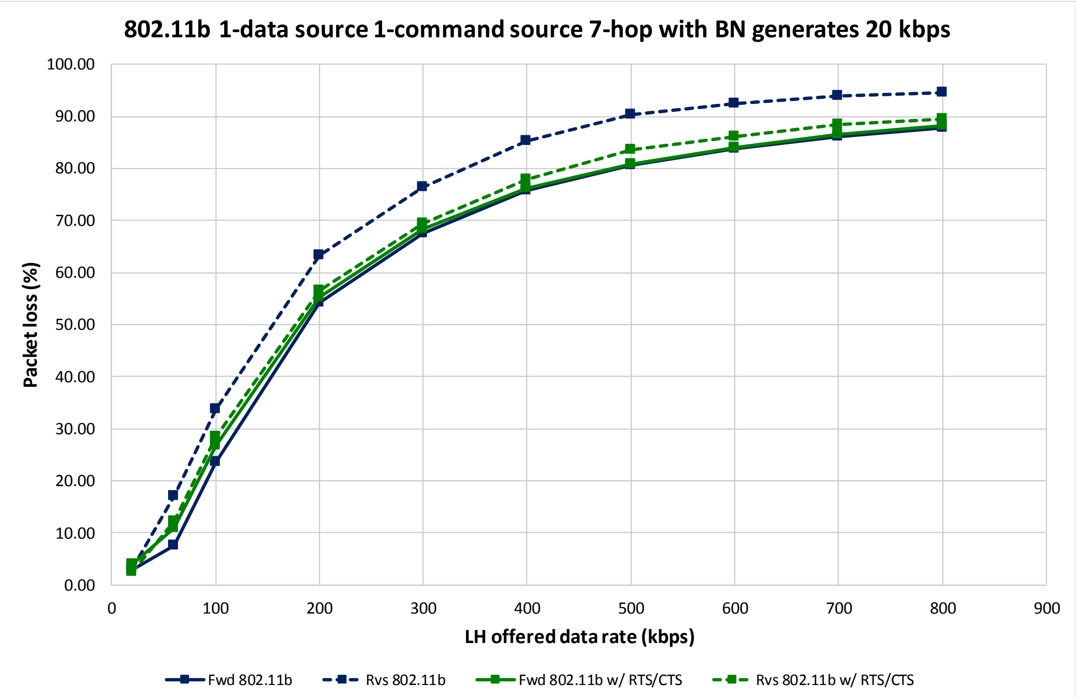

Figure 5-31 Packet loss rate of 802.11b forward and reverse traffics implementing RTS/CTS for priority support, with BN generates 20 kbps

The throughput of reverse and forward traffics for symmetric setting with 2 HCR protocol is shown in Figure 5-32. Reverse traffic throughput rises whilst forward traffic throughput decreases. The amount of reverse traffic throughput rise is proportional to the amount of forward traffic throughput degradation. Furthermore, Figure 5-33 shows that packet delivery rate of reverse traffic increases while packet delivery rate of forward traffic decreases. Similar to the throughput, the amount of packet delivery rise on reverse traffic is comparable to the amount of packet delivery degradation on forward traffic. Moreover, as shown in Figure 5-34, packet loss rate of reverse traffic declines. On the other hand, the packet loss of forward traffic increases

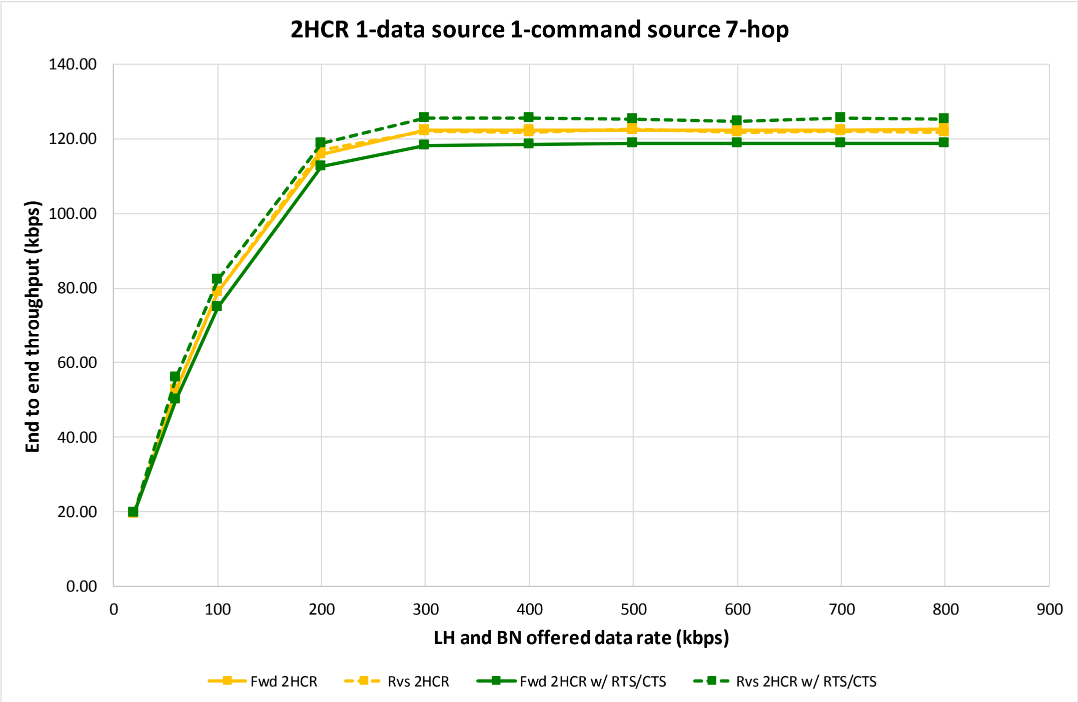

Figure 5-32 Throughput of 2HCR forward and reverse traffics implementing RTS/CTS for priority support

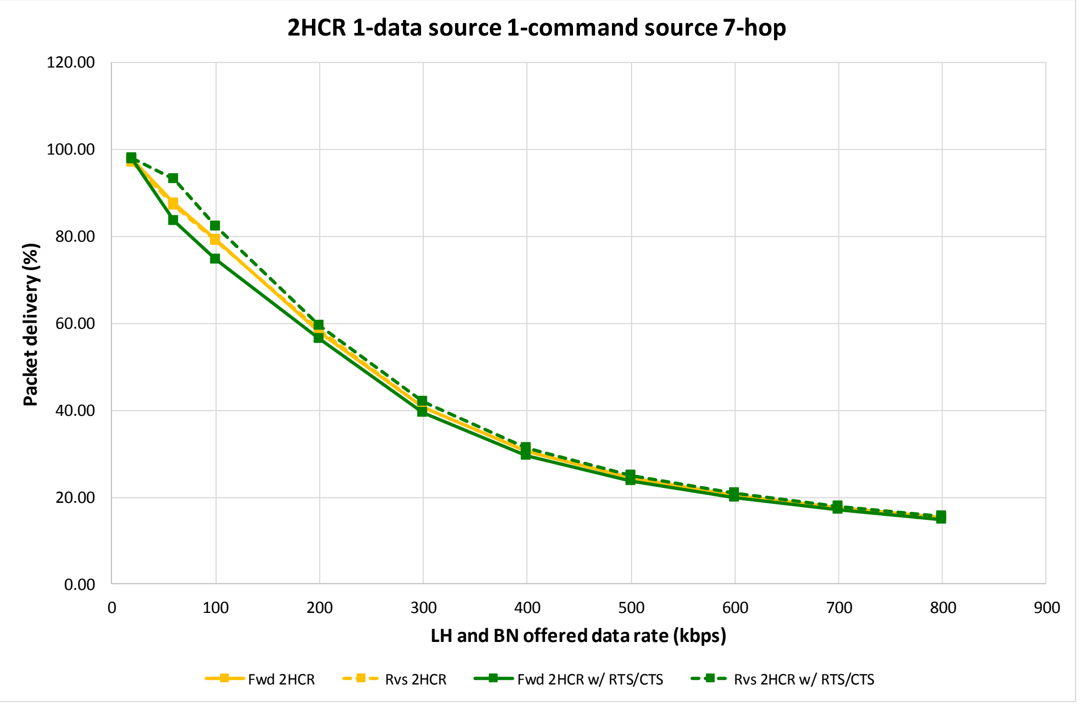

Figure 5-33 Packet delivery rate of 2HCR forward and reverse traffics implementing RTS/CTS for priority support

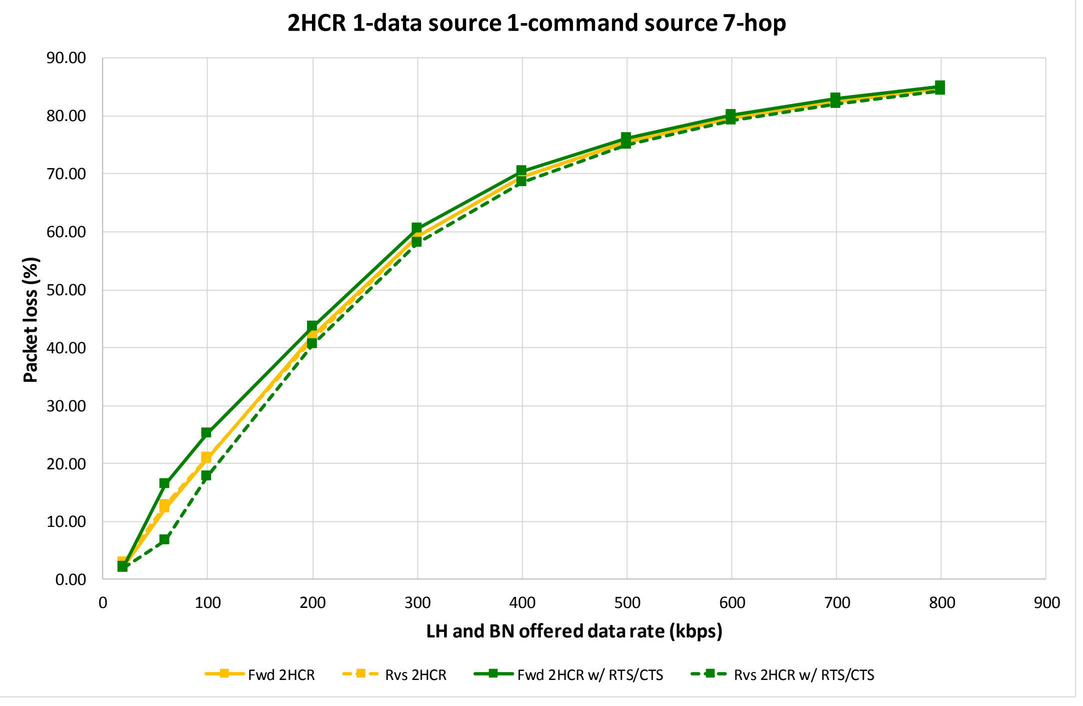

Figure 5-34 Packet loss rate of 2HCR forward and reverse traffics implementing RTS/CTS for priority support

For asymmetric setting with 2HCR, the throughput of reverse and forward traffic is depicted in Figure 5-35. With the use of RTS/CTS on reverse traffic, the throughput of reverse traffic increases while the throughput of forward traffic declines. It shows that RTS/CTS mechanism supressed the throughput of forward traffic. Furthermore, packet delivery rates of reverse and forward traffics are shown in Figure 5-36. Reverse traffic packet delivery rate is significantly improved. However, the packet delivery of reverse traffic is still lower than that of forward traffic. A possible reason is because RTS packet still faces a significant contention with DATA packet. Hence, a modification is required to enhance the performance of this RTS/CTS scheme. Furthermore, as packet delivery rate of reverse traffic increases, its packet loss rate declines as shown in Figure 5-37. On the other hand, packet loss rate of forward traffic increases as its packet delivery rate increases.

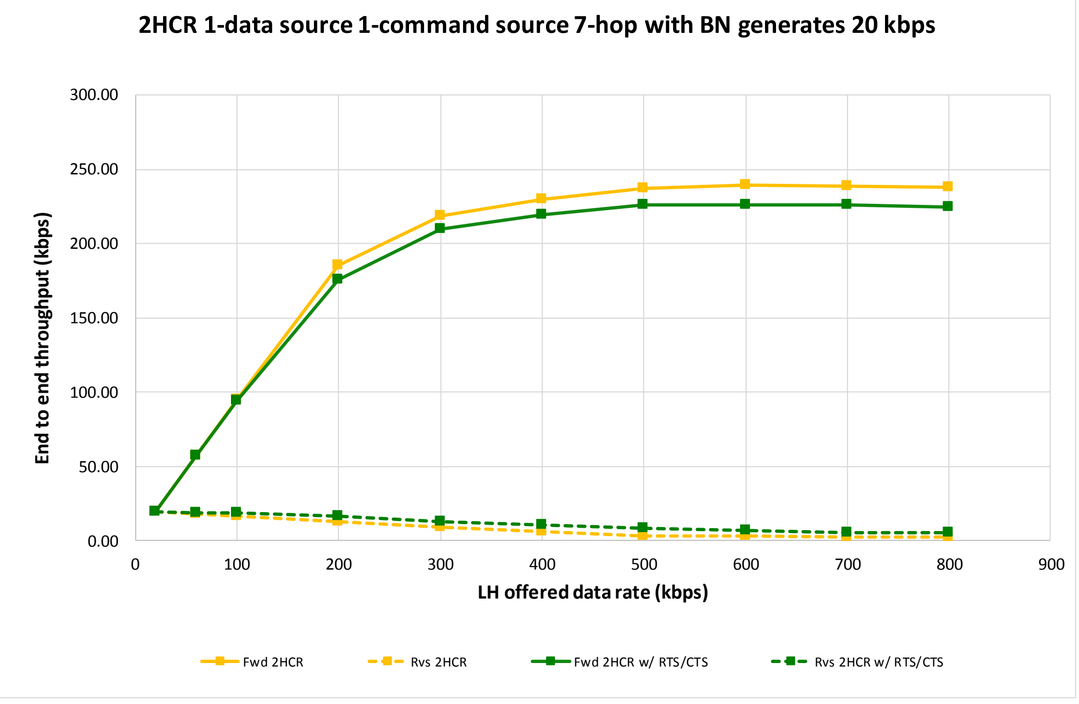

Figure 5-35 Throughput of 2HCR forward and reverse traffics implementing RTS/CTS for priority support, with BN generates 20 kbps

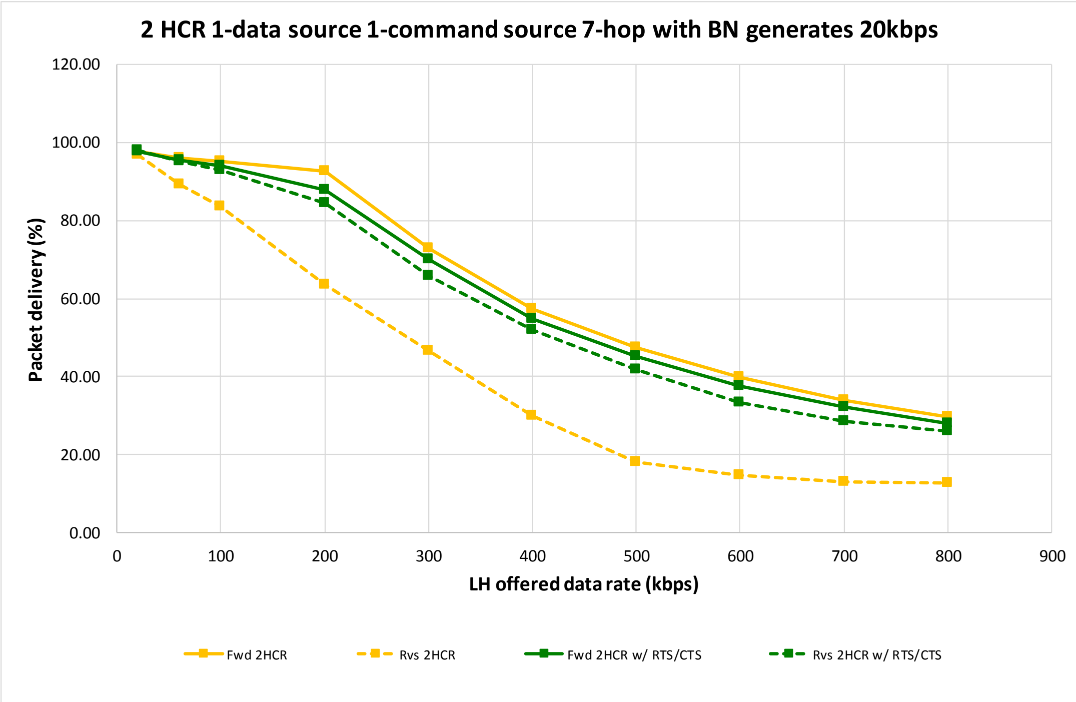

Figure 5-36 Packet delivery rate of 2HCR forward and reverse traffics implementing RTS/CTS for priority support, with BN generates 20 kbps

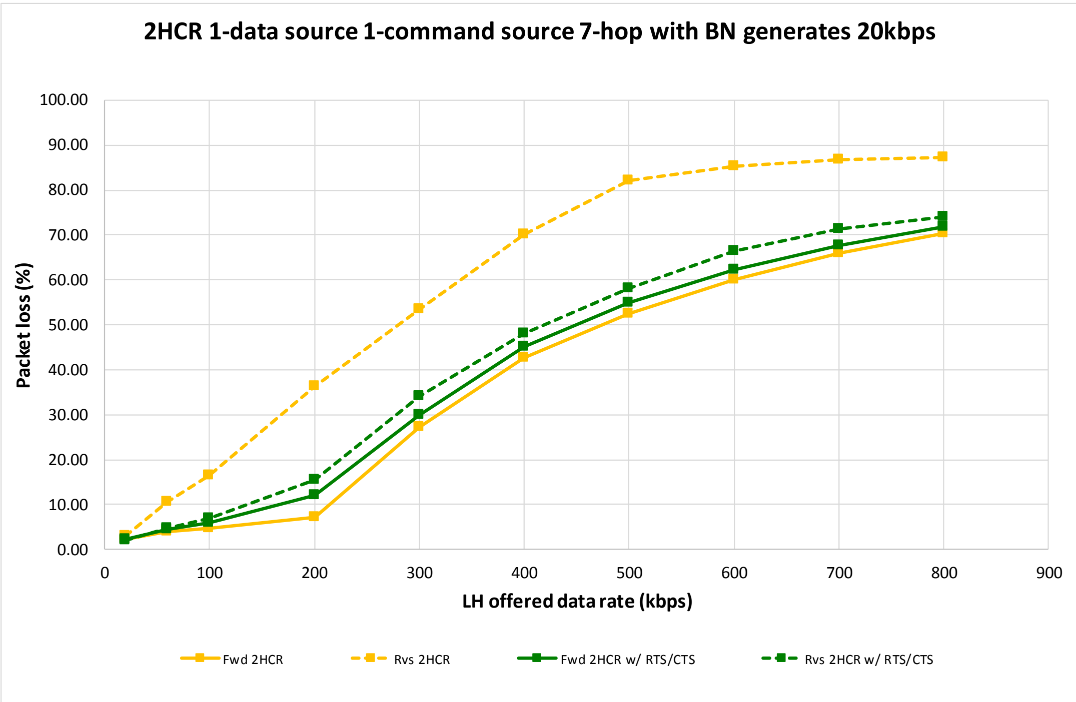

Figure 5-37 Packet loss rate of 2HCR forward and reverse traffics implementing RTS/CTS for priority support, with BN generates 20 kbps

5.5 SIMPLE PRIORITY SUPPORT IN BIDIRECTIONAL TRAFFIC

Previous sections have showed that the use of 802.11e or RTS/CTS protocols for priority support can increase the reverse traffic packet delivery rate when competing with forward traffic. The 802.11e protocol provides a high priority for reverse traffic by assigning IFS and CW that are shorter than those of forward traffic. With such a shorter IFS and smaller CW, reverse traffic can access the channel earlier than forward traffic, and therefore deliver a packet successfully without colliding with forward traffic. Meanwhile, by applying RTS/CTS protocol for reverse traffic, it is shown that the throughput of forward traffic could be supressed, and thus giving more time space for a successful transmission of a reverse traffic packet. Unfortunately, these mechanisms could not work properly in asymmetric setting where the data rate of forward traffic is higher than that of reverse traffic. The simulation results show that packet delivery rate of reverse traffic is still lower than the packet delivery rate of forward traffic. The shorter waiting time provided by 802.11e for reverse traffic, and forward traffic suppression provided by RTS/CTS protocol are not sufficient to lift reverse traffic packet delivery rate above the forward traffic packet delivery rate. Hence, another priority support so called a simple priority support is proposed in this section. The description of this priority support is addressed in Section 5.5.1, while its performance evaluation is discussed in Section 5.5.2.

5.5.1 The Description of Simple Priority Support Scheme

Although the use of shorter IFS and CW by 802.11e and forward traffic suppression by RTS/CTS protocol could not make reverse traffic packet delivery rate higher than forward traffic packet delivery rate, both strategies may derive an advantage if they are combined. Regarding the results in Section 5.4.3, supressing forward traffic could increase packet delivery rate of reverse traffic significantly, and even make it only slightly below the packet delivery rate of forward traffic. This result is achieved in a condition where reverse and forward traffics hold the same IFS, i.e. DIFS, before they start their transmissions. In this case, reverse traffic holds DIFS period before an RTS transmission, as shown in Figure 5-25, while forward traffic holds DIFS period before a DATA packet transmission. Consequently, both packets have the same chance in accessing the channel. Considering this condition, the chance of RTS packet in accessing the channel could be increased by assigning the RTS packet with a shorter IFS. Therefore, we assign point coordination function interframe space (PIFS) for the RTS packet before its transmission while DATA packet keeps using DIFS. For comparison, DIFS has a length of SIFS + 2 x slot time, whilst PIFS has a length of SIFS + slot time. As all protocols studied in this thesis use SIFS of 10 micro seconds and slot time of 20 micro seconds, the length of DIFS and PIFS equal to 50 micro seconds and 30 micro seconds respectively. The pseudocode of simple priority support is shown in Figure 5-38.

A transmission process of a node sending packets in bidirectional traffic depends on type of packet waiting to be sent. There are two types of packets: DATA and COMMAND packets. If a node is sending a DATA packet, it first waits for a DIFS period. Afterwards, the node sends the DATA packet and waits for ACK. If ACK message is received, the process is completed. Otherwise, if ACK is not received within a specified period, DATA packet is resent until the transmission times reach a specified attempt number. On the other hand, the DATA packet will be dropped if it has been retransmitted in such a specified attempt number. Meanwhile, if a node has a COMMAND packet waiting to be sent, it waits for PIFS period, and then sends a RTS packet. Subsequently, the node waits for CTS packet. Once CTS packet is received, the node transmits COMMAND packet. Otherwise, if CTS packet is not received within a specified period, RTS is resent as long its retransmission attempt is less than a specified number. Furthermore, once a COMMAND packet has been transmitted, node waits for ACK packet. If ACK is received, the process is complete. On the other hand, if ACK is not received within a specified period, RTS is retransmitted. In this case, RTS can be resent if its retransmission is less than a specified attempt. Our simple priority support mechanism can be applied to both 802.11b and 2 HCR.

```
Monitoring channel;

if (Send DATA) {          //DATA packet
        Hold for DIFS;
        Send DATA;
        Wait for ACK;
        if (Receive ACK) {
                Process complete ;
                }
        else {
                if (DATA is resent < n times) {
                        GOTO Hold for DIFS ;
                        }
                else {
                        Drop DATA;
                        }
                }
        }

else {                                        // COMMAND packet
        Hold for PIFS;
        Send RTS;
        Wait for CTS;
        if (Receive CTS) {
                Hold for SIFS;
                Send COMMAND;
                Waif for ACK;
                if (Receive ACK) {
                        Process complete ;
                        }
                else {
                        if (RTS is resent < n times) {
                                GOTO Hold for PIFS;
                                }
                        else {
                                Drop RTS and COMMAND;
                                }
                        }
                }
        else {              // does not receiver CTS
                if (RTS is resent < n times) {
                        GOTO Hold for PIFS;
                        }
                else {
                        Drop RTS and COMMAND;
                        }
                }
        }
```

Figure 5-38 Pseudocode of simple priority support scheme

5.5.2 Performance Evaluation of Simple Priority Support Scheme

For symmetric situation, where the data rate of forward and reverse traffic is the same, the throughput of reverse and forward traffics with 802.11b is shown in Figure 5-39. The throughput of reverse traffic increases while the throughput of forward traffic decreases. Similar with the results of symmetric situation in previous sections, the amount of reverse traffic rise is proportional to the amount of forward traffic throughput degradation. The rise of reverse traffic throughput improves its packet delivery rate by the amount that is proportional to the amount of forward traffic packet delivery degradation, as shown in Figure 5-40. As a result, packet loss rate of reverse traffic decreases as depicted in Figure 5-41. Meanwhile, packet loss rate of forward traffic increases.

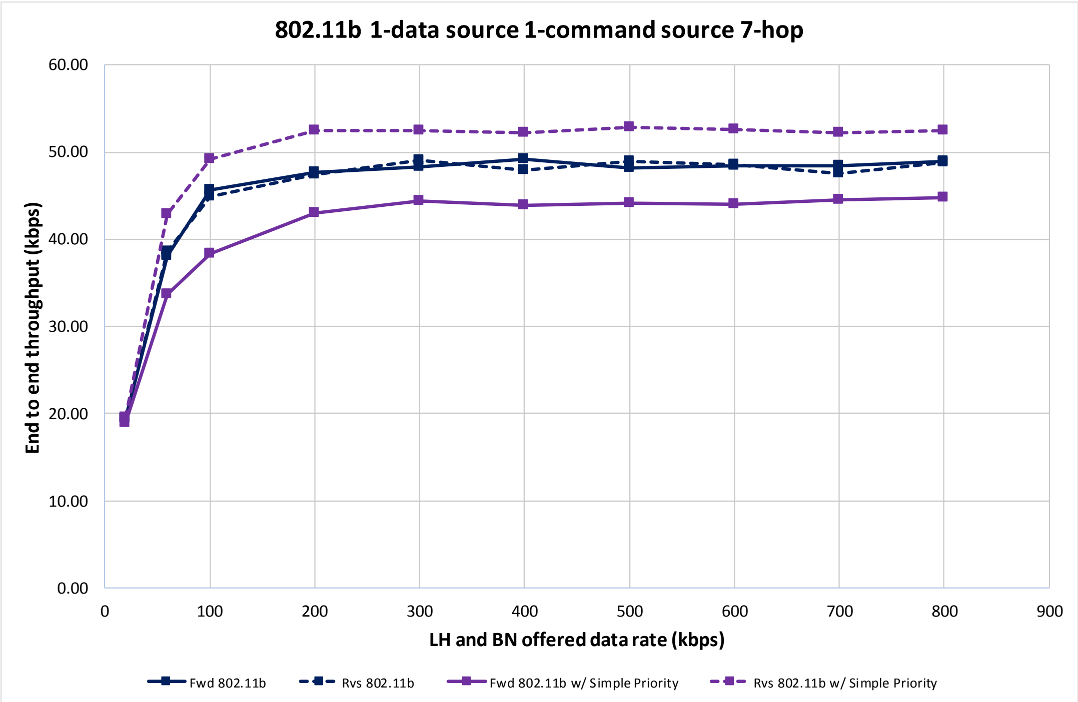

Figure 5-39 Throughput of 802.11b forward and reverse traffics implementing simple priority support

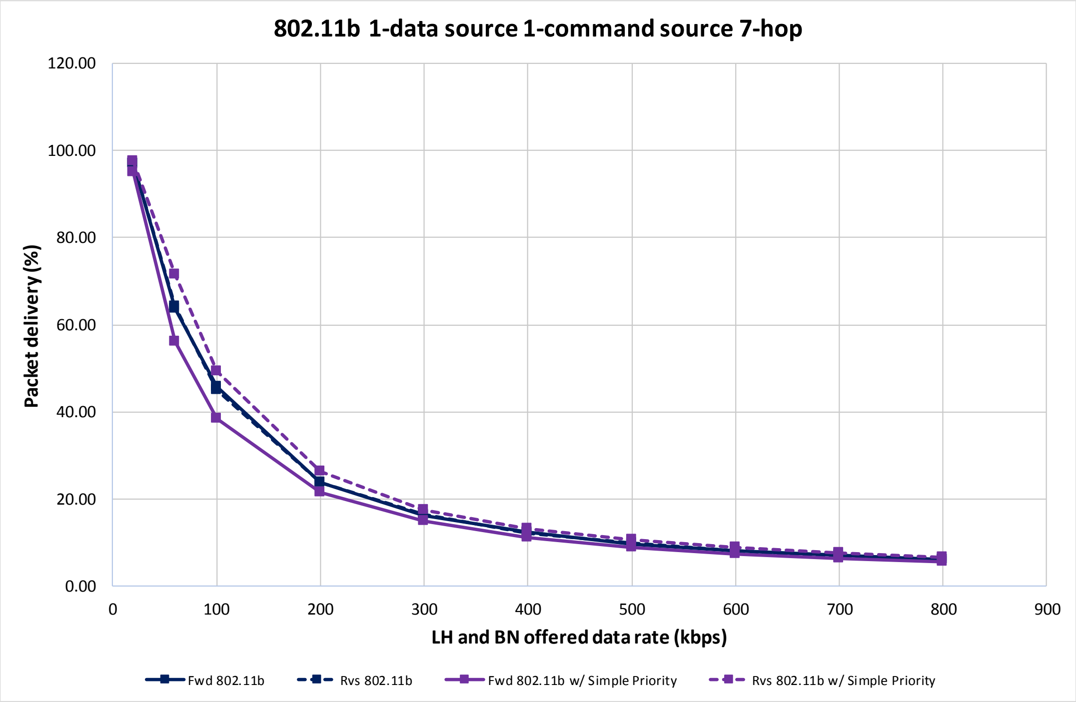

Figure 5-40 Packet delivery rate of 802.11b forward and reverse traffics implementing simple priority support

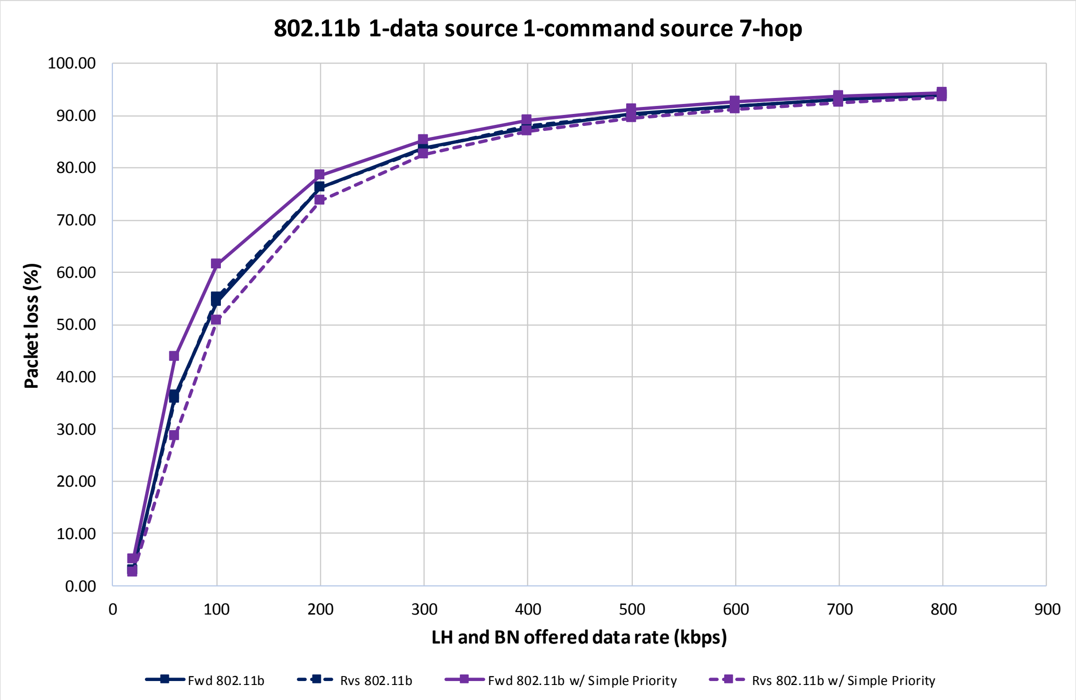

Figure 5-41 Packet loss rate of 802.11b forward and reverse traffics implementing simple priority support

In the case of asymmetric situation with 802.11b protocol, the throughput of forward and reverse traffic is shown in Figure 5-42. Throughput of reverse traffic increases whereas the throughput of forward traffic decreases. It can be seen that the amount of reverse traffic throughput rise is slightly smaller than the amount of forward traffic throughput declination. It can be seen that the reverse traffic packet delivery rate is significantly improved and higher than the forward traffic, which has packet delivery rate decreased slightly, as shown in Figure 5-43. Furthermore, packet loss rate of reverse traffic decreases along with the increase of its packet delivery rate as shown in Figure 5-44. On the other hand, packet loss rate of forward traffic increases as its packet delivery rate degrades. Thus, it can be seen that the simple priority support scheme can achieve the objective of this chapter.

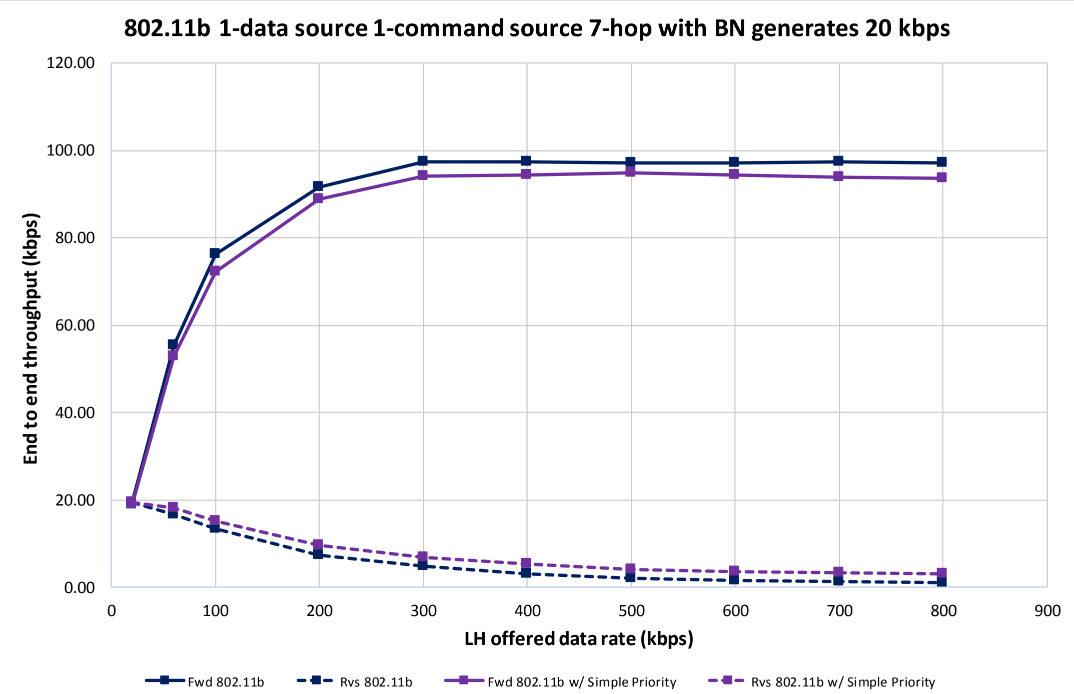

Figure 5-42 Throughput of 802.11b forward and reverse traffics implementing simple priority support, with BN generates 20 kbps

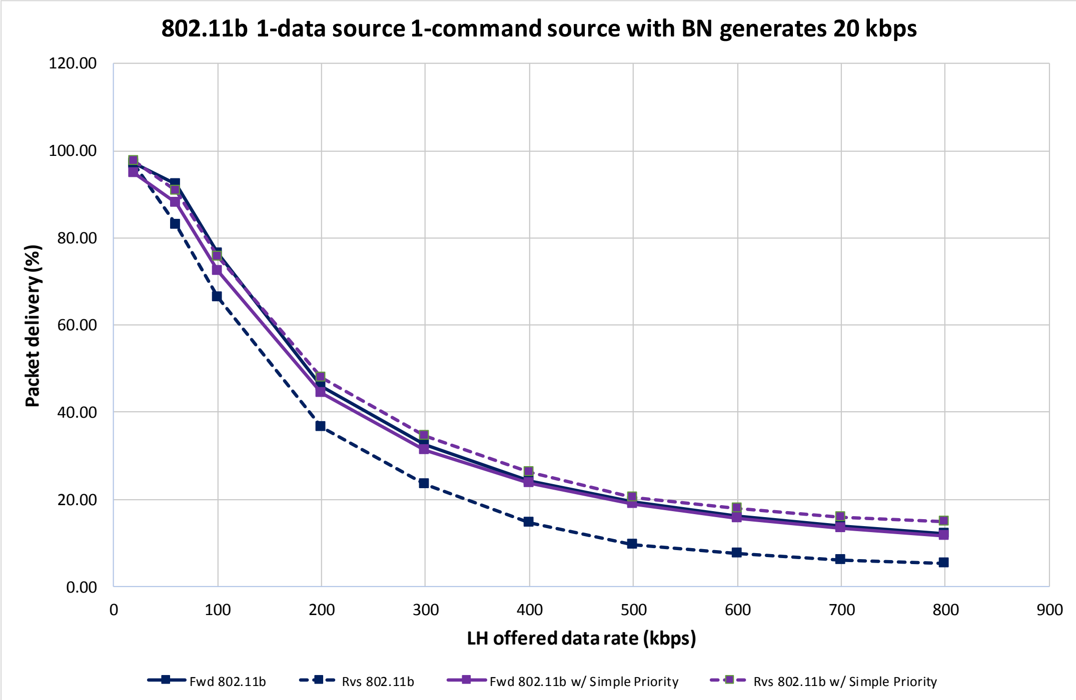

Figure 5-43 Packet delivery rate of 802.11b forward and reverse traffics implementing simple priority support, with BN generates 20 kbps

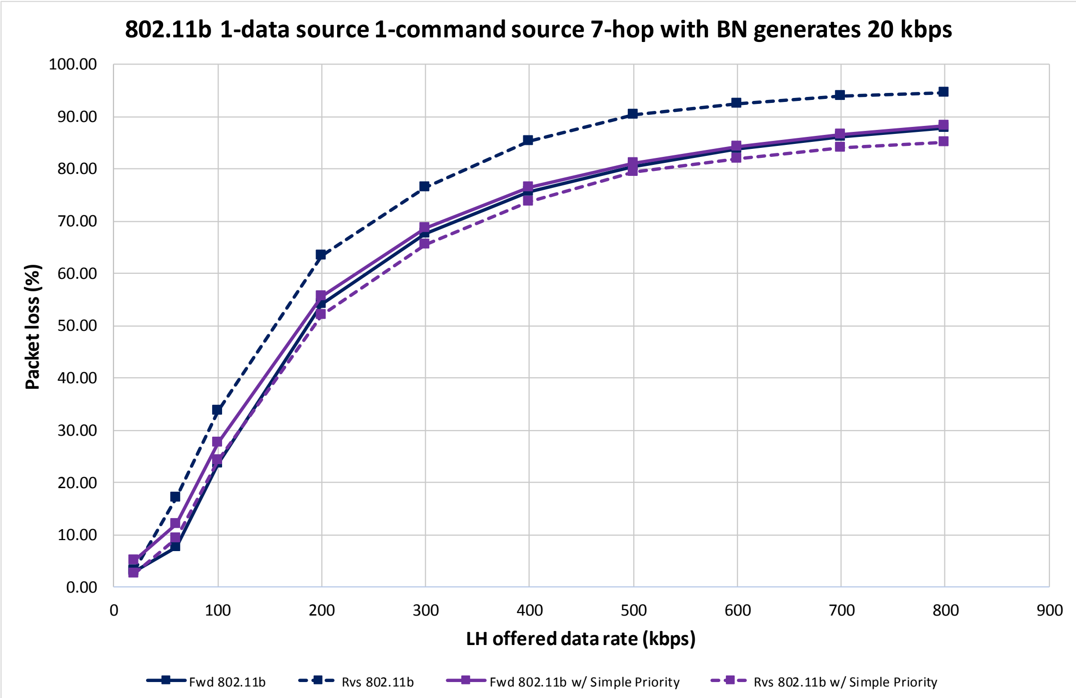

Figure 5-44 Packet loss rate of 802.11b forward and reverse traffics implementing simple priority support, with BN generates 20 kbps

Meanwhile, the throughput of forward and reverse traffics for symmetric situation with 2HCR protocol is shown in Figure 5-45. Again, the throughput of reverse traffic rises whereas the throughput of forward traffic declines. The rise of reverse traffic throughput is proportional to the degradation of forward traffic throughput. Similarly, packet delivery rate of reverse traffic increases while packet delivery rate of forward traffic decreases, and reverse traffic packet delivery is higher, as shown in Figure 5-46. Moreover, Figure 5-47 shows packet loss rates of both reverse and forward traffics. It can be seen that packet loss rate of reverse traffic decreases as its packet delivery increases. In contrast, packet loss rate of forward traffic increases as its packet delivery declines.

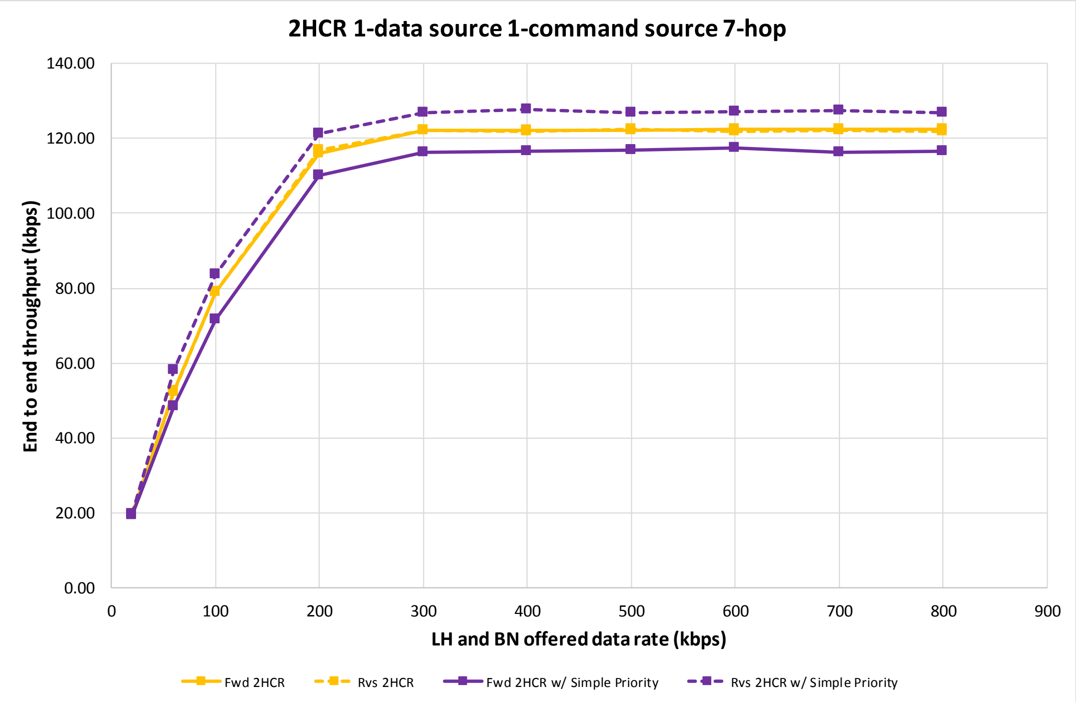

Figure 5-45 Throughput of 2HCR forward and reverse traffics implementing simple priority support

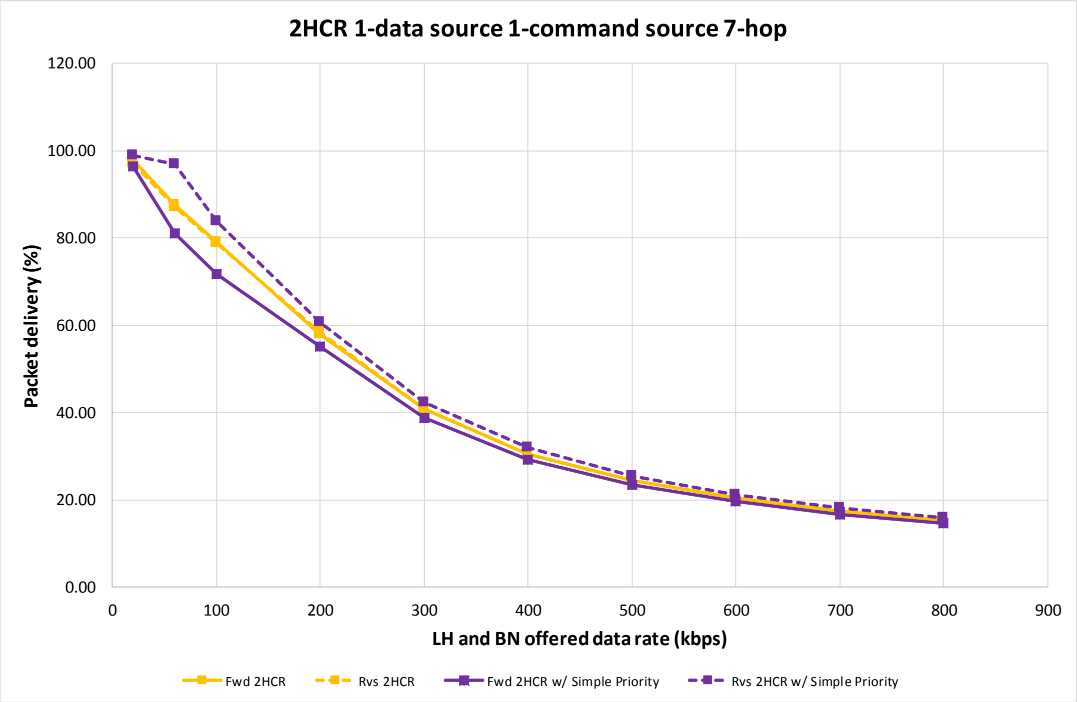

Figure 5-46 Packet delivery rate of 2HCR forward and reverse traffics implementing simple priority support

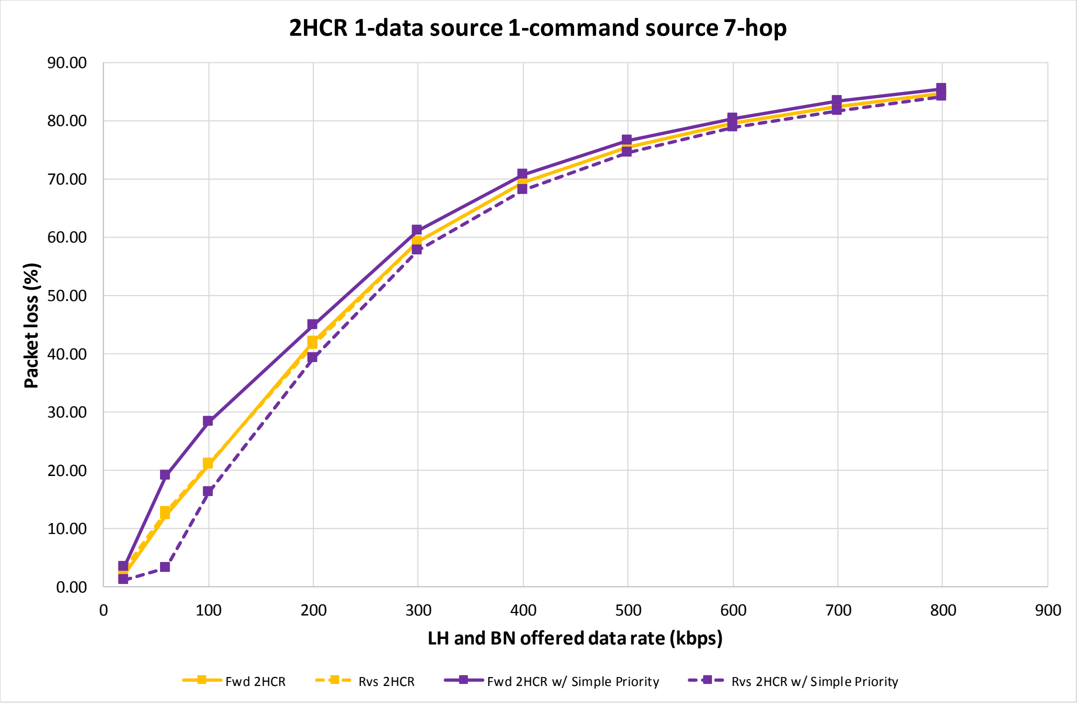

Figure 5-47 Packet loss rate of 2HCR forward and reverse traffics implementing simple priority support

Finally, the throughput of forward and reverse traffics for asymmetric situation with 2HCR protocol is shown in Figure 5-48. The throughput of reverse traffic increases whereas the throughput of forward traffic degrades. The rise of reverse traffic throughput is lower than the degradation of forward traffic throughput. However, such throughput increase is enough to make reverse traffic packet delivery rate higher than forward traffic delivery rate, as shown in Figure 5-49. The forward traffic packet delivery only reduces slightly. Moreover, packet loss rates on reverse and forward traffics are shown in Figure 5-50. The packet loss rate of reverse traffic decreases while the packet loss of forward traffic increases.

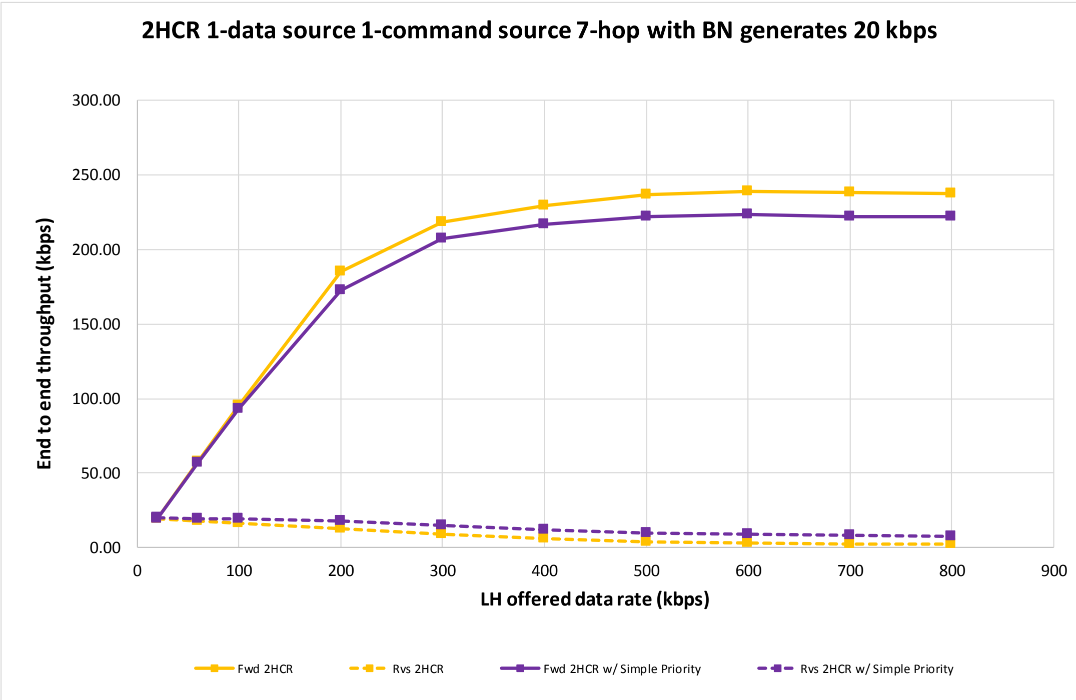

Figure 5-48 Throughput of 2HCR forward and reverse traffics implementing simple priority support, with BN generates 20 kbps

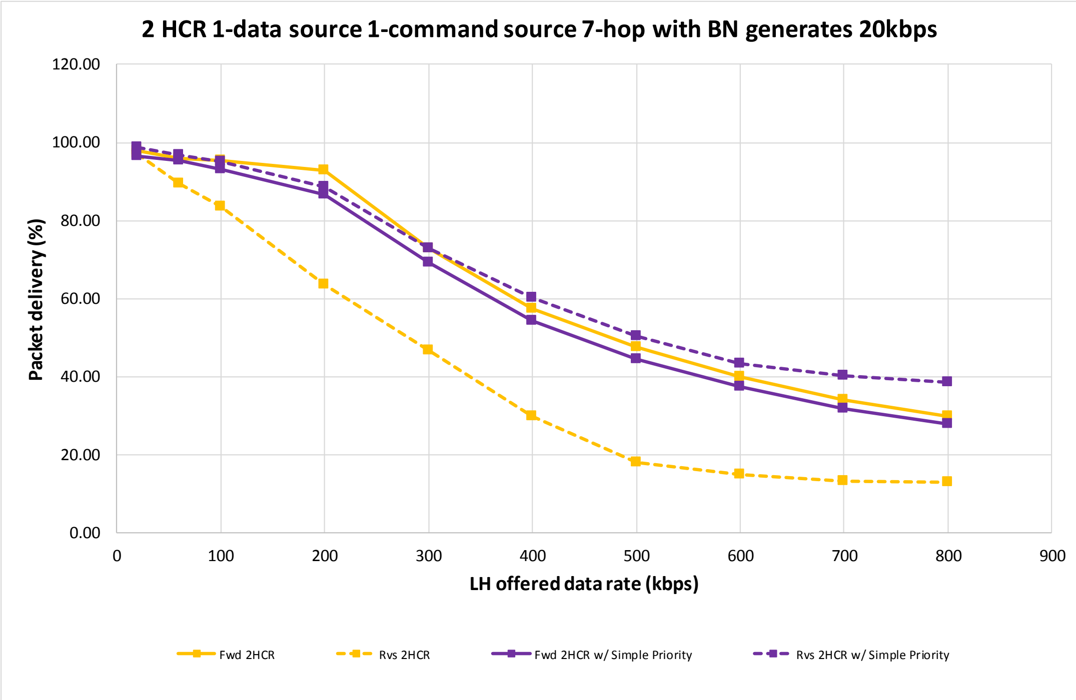

Figure 5-49 Packet delivery rate of 2HCR forward and reverse traffics implementing simple priority support, with BN generates 20 kbps

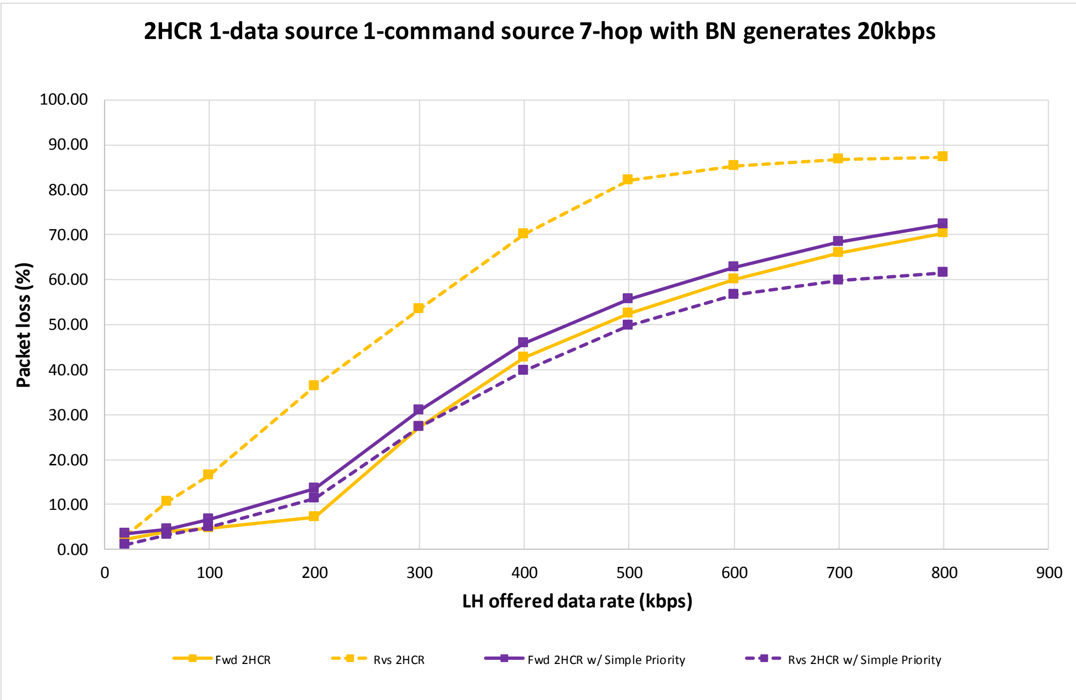

Figure 5-50 Packet loss rate of 2HCR forward and reverse traffics implementing simple priority support, with BN generates 20 kbps

5.6 SUMMARY

In this chapter, it is first examined the performance of 2HCR protocol in bidirectional traffic scenario for both symmetric and asymmetric settings. It is found that 2HCR still outperforms 802.11b and MC CSMA. It is also observed that both directions receive more or less the same treatment in symmetric setting. However, COMMAND traffic receives lower packet delivery rate in symmetric setting in all examined protocols. Considering that reverse traffic has an important role in carrying messages for remote network supervisory and management, a higher priority in accessing the shared channel must be given to this traffic. The purpose of this priority treatment is to provide reverse traffic packet delivery rate that is higher than forward traffic packet delivery rate, particularly in a situation where data rate of reverse traffic is significantly lower than the data rate of forward traffic.

The first effort is by using the existing 802.11e quality of service (QoS). However, the simulation results show that this scheme does not give a significant improvement, particularly for the asymmetric situation where the data rate of reverse traffic is significantly below the data rate of forward traffic. Then, another strategy is developed to give reverse traffic a better priority. It can be achieved by suppressing forward traffic throughput with the use of RTS/CTS packet prior reverse traffic packet transmission. This method gives a better performance compare with the performance derived by 802.11e scheme. However, packet delivery rate of reverse traffic is still below the packet delivery rate of forward traffic. It may be due to the same IFS used in both reverse and forward traffic. Therefore, a simple priority support is proposed to solve the problem. This scheme combines the use of RTS/CTS for reverse traffic with the utilization of shorter IFS and smaller CW. The simulation result shows that this method could derive the best priority support enhancement compared with the previous methods, and can provide reverse traffic packet delivery rate that is higher than the forward traffic packet delivery rate.

CHAPTER 6

CONCLUSIONS AND FUTURE WORKS

6.1 CONCLUSIONS

In several wireless sensor network (WSN) applications, groups of sensor nodes (SNs) are distributed across a huge area located in a rural region separated hundreds kilometres away from the control station (CS). As telecommunications infrastructure is generally not available in rural areas, it would be worthwhile to consider the use of a dedicated WSN network.

In this thesis, a three-tier dedicated WSN network is utilized to provide connections between a high number of SNs clusters, that are mostly located in rural area, and CS located in the capital city. In three-tier architecture, networks in Tier 2 and Tier 3 are configured by a large number of multi-hop networks in the form of chain and tree topologies. As it is well known that multi-hop networks suffer from throughput degradation due to hidden and exposed node problems, a multichannel MAC so called 2-hop channel reservation (2HCR), is proposed to enhance the performance of these specific multi-hop networks. In 2HCR, the effects of hidden node and exposed node problems are reduced by attempting nodes located 2 hops away to use different channel. Performance of 2HCR is evaluated using computer simulation and compared with the performance of 802.11b and multichannel CSMA (MC MAC) protocols.

Furthermore, it is common to estimate the performance of a network by using computer simulation. Based on this method, various estimation methods have been proposed. Several methods examined in this thesis are not suitable with the requirement. They tend to be complex if they are used to predict networks with irregular tree topology available in Tier 2 and Tier 3. Therefore, an estimation method using a simple mathematical operation is proposed in this thesis. The advantage of this simple method is its ability in deriving a fast prediction result, if the estimation is undertaken in the field, where the topology may often change. To evaluate this method accuracy, the estimation result is compared with the simulation result. The estimation and its evaluation are performed for 2HCR, MC CSMA and 802.11b protocols.

Moreover, as the WSN studied in this thesis is intended to provide network supervisory and management, another traffic carrying command packets is provided to complement the existing traffic carrying data packets. While the existing traffic so called forward traffic is generated SNs to be sent to CS, the additional traffic so called reverse traffic is generated by CS to be sent to SNs or other nodes. This bidirectional traffic could affect the performance of 2HCR protocol, and therefore this protocol is evaluated under bidirectional traffic. As well as in previous unidirectional traffic, performance of 2HCR is compared with the performance of 802.11b and MC CSMA protocols. Also, due to the important role of reverse traffic in providing successful network supervisory and management, the reverse traffic is desired to have a better packet delivery rate than forward traffic. For this reason, a simple priority support is proposed to give reverse traffic a high priority in accessing the channel resource.

Following the extensive investigations described in the previous chapters of this thesis, these concluding remarks are made:

- To provide an early warning system for a huge observation area such as in the province of East Kalimantan, Indonesia, an environmental WSN studied in this thesis comprises a high number of SNs clusters that are deployed sparsely within the region. To establish communication link between SNs clusters and the CS located hundreds kilometres away, Chapter 3 proposed a three-tier WSN architecture. In this architecture, Tier 1 provides data measurement and collection whereas Tier 3 works as a long haul communication link connecting rural areas and the capital city. Meanwhile, Tier 2 connects Tier 1 and Tier 3 as the distance between Tier 1 and Tier 3 still far. Each tier has a specified frequency that is different with the other tier frequency. To interface different tiers, a specified node is equipped with two transceivers. For instance, a local head (LH) that is a head in an SNs cluster, collects data from

SNs through radio for Tier 1, and then forwards the data to a relay node (RN) by using radio for Tier 2. Numbers of RNs forward the data to a local backbone node (BN). Similar with LH, (BNs) perform inter-tier interfacing between Tier 2 and Tier 3. Upon receiving data forward RN, BN then delivers the data to the CS. Networks in all tiers configure multihop communication. Furthermore, while networks in Tier 1 can be in tree, chain, or mess topologies, networks in Tier 2 and Tier 3 could be in the form of long chain and irregular tree topologies comprising long chains. This network architecture is considered able to adapt to topology change and scalability.

- To enhance the throughput of multihop networks particularly those in Tier 2 and Tier 3, a two-channel medium access control so called 2HCR is developed in Chapter 3. The purpose of 2HCR is to prevent nodes two hops away using the same transmission channel. With this method, collision due to hidden node could be avoided, while simultaneous transmissions in the presence of exposed node could be enabled. As a result, the throughput of multihop network can be enhanced. To evaluate the performance of 2HCR, a computer simulation is conducted in various topologies. The same simulation is also provided for 1 channel 802.11b and 2 channels MC CSMA protocols for performance comparison. The simulation is performed with and without RTS/CTS handshake. Regarding the simulation result, the throughput obtained by 2HCR is higher than the throughput obtained by 802.11b and MC CSMA, for all topologies and conditions we have considered.

- A simple throughput estimation method is also developed in Chapter 4 of this thesis. The estimation is performed by iteratively decomposing the complex network until the last topology is the same with as one of the basic topologies. During the decomposition of a complex topology into the simplest topology, the throughput of the network in each process is obtained by using the throughput of respected basic topology. The estimation method has been applied with 2HCR, MC CSMA, and 802.11b MACs, with and without a RTS/CTS mechanism, and compared with simulation results. Most of the estimation results give a deviation of less than 10 %. It shows that such a simple estimation method can give the accurate results.

- In Chapter 5, the performance of 2HCR is evaluated in the presence of bidirectional traffic comprising an additional reverse traffic and the existing forward traffic. The performance of 802.11b and MC CSMA protocol is also evaluated for comparison. The results in Section 5.1 show that 2HCR still outperforms 802.11b and MC CSMA protocols.

- Further evaluation for 2HCR and 802.11 is also provided in Chapter 5. The purpose of this evaluation is to observe packet delivery rate of reverse and forward traffic under two situations. In symmetric situation, the data rate of reverse and forward traffic is generated similarly. On the other hand, in asymmetric situation, the data rate of reverse traffic is lower than that of forward traffic. For the symmetric situation, the results show that the packet delivery of reverse traffic is similar with the packet delivery of forward traffic. For the asymmetric situation, however, packet delivery of reverse traffic is lower than that of forward traffic. As it is desired that packet delivery of reverse traffic is higher than packet delivery of forward traffic, three attempts are provided in this chapter. In Section 5.3, the existing 802.11e priority protocol is implemented in bidirectional traffic network. Despite this method increases packet delivery of reverse traffic, in asymmetric setting, this improvement could not derive reverse traffic packet delivery rate that is higher than forward traffic packet delivery rate. Another approach then is proposed in Section 5.4. In this section, RTS/CTS protocol is implemented only on reverse traffic to suppress the throughput of forward traffic. This method provides a better enhancement than that attempted by 802.11e protocol. Nevertheless, for the symmetric setting, packet delivery rate of reverse traffic is still below packet delivery rate of forward traffic. As such, a simple priority support scheme is proposed in Section 5.5. This method combines the advantage of RTS/CTS and 802.11e protocols. The results show that the proposed scheme is able to provide reverse traffic packet delivery rate higher than forward traffic packet delivery rate.

6.2 FUTURE WORKS

The results of this intensive study show potential for further development. Therefore, the following recommendations for future work are made:

- 2HCR MAC is proven able to improve the performance of multi-hop networks with the chain and tree topologies, even though working only on two different channels. However, the observation on simple tree topologies, i.e. chain topology with branches, found that collision still happens in the branches. Therefore, to reduce the collisions between nodes in the branches, particularly consecutive branches that can exist in the real network, more one or two channels may be introduced to improve the network throughput. Additional channels can also reduce the probability of "one channel idle" situation that leads to packet collision in a high input data rate.

- Even though the proposed estimation method derives prediction results with deviation mostly less than 10%, the deviations higher than 10 % also occurs. It is possibly because decomposition procedure ignores the relation between sub-networks. Therefore, to enhance the accuracy of the estimation result, further investigation on sub-network relation could be conducted to find the transformation model of this relation. The choice on other structures of basic topologies may be able to solve this problem.

- In this research, the throughput of basic topologies is derived from the simulation result. To estimate the throughput of a real network in a specified area, the throughput of basic topologies may be obtained from a real measurement. By means of the empirical results, more factors affecting the estimation accuracy could be derived to improve the ability of the estimation method in a specified target area.

REFERENCES

[1]. T. Alhmiedat, A. A. Taleb, and M. Bsoul, "A study on threats detection and tracking systems for military application using WSNs", in *International Journal of Computer Applications 40 (15)*, Feb. 2012, pp. 12-18.

[2]. L. Lamont, M. Toulgoat, M. Deziel, and G. Patterson, "Tiered wireless sensor network architecture for military surveillance applications", in *Proceeding of The Fifth International Conference on Sensor Technologies and Applications"*, Canada, 2011, pp. 288-294.

[3]. S. Kim, "*Wireless sensor networks for structural health monitoring*", Research project of Dept. of electrical Engineering and Computer Science, University of California at Berkeley, 2005.

[4]. B. Alphenaar, "*Wireless sensor network for electric transmission line monitoring*", Final Technical Report, University of Louisville, January 2010.

[5]. L. Bencini, D. Di Palma, G. Collodi, G. Manes, and A. Manes, "Wireless sensor networks for on-field agricultural management process", in *Wireless Sensor Networks: Application-Centric Design,* edited by: Y. K. Tan, InTech, Rijeca, Croatia, 2010, pp. 1-18.

[6]. S. A. Sawant, J. Adinarayana, S. S. Durbha, A. K. Tripathy, and D, Sudharsan, "Service oriented architecture for wireless sensor networks in agriculture", in *International Archives of the Photogrametry, Remote Sensing and Spatial Information Sciences, XXXIX-B4*, 2012, pp. 467-472.

[7]. R. Jafari, A. Encarnacao, A. Zahoory, F. Dabiri, H. Noshadi, and M. Sarrafzadeh, "Wireless sensor networks for health monitoring", in *Proceeding of The Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services 2005 (MobiQuitous 2005)*, San Diego, USA, July 17-21 2005, pp. 479-481.

[8]. K. K. Khedo, R. Perseedoss, and A. Mungur, "A wireless sensor network air pollution monitoring system", in *International Journal of Wireless & Mobile Networks (IJWMN) 2 (2)*, May 2010, pp. 31-45.

[9]. A. Mainwaring, J. Polastre, R. Szewczyk, D. Cullen, and J. Anderson, “Wireless sensor networks for habitat monitoring, in *Proceeding of Wireless Sensor Networks and Applications 2002 (WSNA ’02)*, Atlanta, USA, September 28 2002.

[10]. G. Werner-Allen, K. Lorincz, M. Welsh, O. Marcillo, J. Johnson, M. Ruiz, and J. Lees, “Deploying a wireless sensor network on active volcano”, in *IEEE Internet Computing*, March-April 2006, pp. 18-25.

[11]. K. Mikhaylov, J. Tervonen, J. Heikkila, and J. Kansakoski, “Wireless sensor networks in industrial environment: real-life evaluation result”, in *Proceeding of The 2nd Baltic Congress on Future Internet Communications (BCFIC),* Vilnius, Lithuania, April 25-27 2012, pp. 1-7.

[12]. A. Low, “Evolution of wireless sensor networks for industrial control”, in *Technology Innovation Management*, May 2013, pp. 5-12.

[13]. J. M. Bohli, A. Hessler, O. Oguns, and D. Westhoff, “A secure and resilient WSN roadside architecture for intelligent transport system” in *Proceeding of WiSee ’08,* Alexandria, USA, March 31 – Apr 2 2008.

[14]. S. K. Garghan, R. Nordin, and M. Ismail, “A survey on energy efficient wireless sensor networks for bicycle performance monitoring application”, in *Jurnal of Sensor 2014,* pp. 1 – 16.

[15]. N. M. Su, H. Park, E. Bostrom, J. Burke, M. B. Srivastava, and D. Estrin, “Augmenting film and video footage with sensor data”, in *Proceeding of The 2nd IEEE Annual Conference on Pervasive Computing and Communications 2004 (PerCom 2004)*, Orlando, USA, March 14-17 2004, pp. 3-12.

[16]. M. V. Ramesh, S. Kumar, and P. V. Rangan, “Wireless sensor network for landslide detection”, in *Proceeding of The 2009 International Conference of Wireless Network (ICWN09),* Las Vegas, USA, 2009, pp. 13-16.

[17]. C. Hartung, R. Han, C. Seielstand, and S. Holbrook, “FireWxNet: a multi-tiered portable wireless system for monitoring weather conditions in wildland fire environments”, in *Proceeding of International Conference of Mobile Systems, Applications, and Services (MobiSys) 2006”,* Uppsala, Sweden, June 19-22 2006.

[18]. IEEE, "Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications" in *IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific Requirements"*, IEEE Std. 802.11-2007 (Revision of IEEE Std. 802.11-1999), 2007, pp. C1-1184.

[19]. Crossbow Technology, Inc.,"*Mica2 Datasheet*", http://www.xbow.com, accessed on December 14 2009.

[20]. P. Sikka, P. Corke, L. Overs, P Valencia, and T. Wark, "Fleck- a platform for real-world outdoor sensor networks" in Proceeding of IPSN/SPOTS '07, Cambdrige, USA 2007.

[21]. WiSense, "Wisense WSN1120L Datasheet", http://wisense.in/datasheets/ WSN1120L-datasheet.pdf, accessed on May 15 2017.

[22]. P.C. Ng and S.C. Liew, "Throughput analysis of IEEE 802.11 multi-hop ad hoc networks", in *IEEE/ACM Transaction on Networking 15 (1),* 2007.

[23]. S. D. Gunashekar, A. Das, T. Erlebach, and E. M. Warrington, "Wireless multi-hop throughput: preliminary results from a simulation-based study", in *Proceeding of 2011 Loughborough Antennas and Propagation Conference*, Loughborough, UK., Nov. 14-15 2011, pp. 1-4.

[24]. K.N. Ting and M.L. Sim, "Wireless broadband provisioning using single radio multihop wi-fi systems with chain topology", in *Proceeding of The 13th IEEE International Conference on Networks (ICON 2005)* joint held with *2005 IEEE 7th Malaysian Conference on Communication*, Kuala Lumpur, Malaysia, November 16-18 2005, pp. 37-41.

[25]. A. Jayasuriya, S. Perreau, A. Dadej, and S. Gordon, "*Hidden vs exposed terminal problem in ad hoc networks*", http://www.itr.unisa.edu.au/ ~sgordon/doc/ jayasuriya2004 -hidden.pdf.

[26]. K. Kosek-Szott, "A survey of MAC layer solutions to the hidden node problem in ad-hoc networks", in *Ad Hoc Networks 2012 (10)*, Elsevier, pp. 635-660.

[27]. J. Mo, H. W. So, and J. Walrand "Comparison of multichannel MAC protocol", in *IEEE/ACM Transaction on Mobile Computing 7 (1),* 2008.

[28]. O. D. Incel, "A survey on multi-channel communication in wireless sensor networks", in *Computer Networks 2011 (55)*, June 14 2011, pp. 3081-3009.

[29]. S. L. Wu, C. Y. Lin, Y. C. Tseng, and J. P. Sheu, "A new multi-channel MAC protocol with on-demand channel assignment for mobile ad-hoc networks", in *Proceeding of The International Symposium on Parallel Architectures, Algorithms, and Networks 2000 (ISPAN '05)*, Las Vegas, USA, Dec 7 - 9 2005.

[30]. J So, and N Vaidya, "Multi-channel MAC for ad hoc networks: handling multi-channel hidden terminals using a single transceiver", in *Proceeding of The Fifth ACM International Symposium on Mobile AdHoc Networking and Computing 2004 (MobiHoc '04)*, Roppongi, Japan, May 24-26 2004.

[31]. A. Tzamaloukas, and J.J. Garcia-Luna-Aceves, "Channel-hopping multiple access", in *Proceeding of IEEE International Conference on Communication 2000 (ICC 2000)*, New Orleans, USA, June 18 - 22 2000.

[32]. NS3, http://www.nsnam.org, accessed on May 31 2011.

[33]. P. Gupta and P. R. Kumar, "The capacity of wireless networks", in *IEEE Transactions on Information Theory 46(2)*, March 2000, pp. 388-404.

[34]. L. Kleinrock and J. Silvester, "Optimum transmission radii for packet radio networks or why six is a magic number", in *Proceeding of IEEE National Telecommunication Conference, Birmingham, USA*, Dec. 3-6 1978, pp. 4.3.1–4.3.5.

[35]. S. Toumpis and A. J. Goldsmith, "Capacity regions for wireless ad hoc networks, in *IEEE Transactions on Wireless Communications 2(4)*, July 2003, pp. 736-748.

[36]. A. K. Haddad and R, Riedi, "Bounds for the capacity of wireless multihop networks imposed by topology and demand", in *Proceeding of MobiHoc 2007*, Montreal, Canada, Sep. 9-14 2007.

[37]. G. Mergen and L. Tong, "Stability and capacity of regular wireless networks", in *IEEE Trnsactions on Information Theory 15(6)*, June 2005, pp. 1938-1953.

[38]. B. Liu, P. Thiran, and D. Towsley, "Capacity of wireless ad hoc network with infrastructure", in *Proceeding of MobiHoc 2007*, Montreal, Canada, Sep. 9-14 2007.

[39]. IEEE, "Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications, amendment 8: medium access control (MAC) quality of service enhancements" in *IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific Requirements"*, IEEE Std. 802.11e-2 (Amendment to IEEE Std. 802.11-1999 edition), 2005.

[40]. A. Nasipuri, J. Zhuang, and S. R. Das, "A multichannel CSMA MAC protocol for multihop wireless networks", in *Proceeding of Wireless Communication and Networking Conference 1999 (WCNC 1999),* New Orleans, USA, September 21-24 1999.

[41]. D. Hughes, P. Greenwood, G. Blair, G. Coulson, P. Grace, F. Pappenberger, P. Smith, and K. Beven, "An experiment with reflective middleware to support grid-based flood monitoring", in *Concurency and Computation: Practice and Experience 2008 (20),* Willey InterScience, 2008, pp. 1303-1316.

[42]. P. Jiang, H. Xia, Z. He, and Z. Wang, "Design of a water environment monitoring system based on wireless sensor networks", in *Sensors 2009 (9),* August 2009, pp. 6411-6434.

[43]. A. Rosi, M. Berti, N. Bicocchi, G. Castelli, A. Corsini, M. Mamei, and F. Zambonelli, "Landslide monitoring with sensor networks: experiences and lessons learnt from a real-world deployment", in *International Journal of Sensor Networks 10 (3),* 2011, pp. 111-122.

[44]. J. Lee, J. E. Kim, D. Kim, P. K. Chong, J. Kim, and P. Jang, "RFMS: Real-time flood monitoring system with wireless sensor networks", in *Proceeding of The 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems 2008 (MASS2008),* Atlanta, US, Sept. 29-Oct. 2 2008, pp. 527-528.

[45]. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Caryici, "A survey on sensor networks", in *IEEE Communication Magazine*, August 2002, pp 102-114.

[46]. T. Watteyne, "*Energy-Efficient Self-Organization for Wireless Sensor Networks",* PhD Thesis, Institut National des Sciences Appliquees de Lyon, 2008.

[47]. R. Vidhyapriya and P. T. Vanathi, "Energy aware routing for wireless sensor networks", in *Proceeding of IEEE-ICSCN 2007,* Feb. 22-24 2007, pp. 545-550.

[48]. R. Zhu, Y. Qin, and J. Wang, "Energy-aware distributed intelligent data gathering algorithm in wireless sensor networks", in *International Journal of Distributed Sensor Networks 2011*, pp. 1-13.

[49]. B. Jiang, B. Ravindran, and H. Cho, "Energy efficient sleep scheduling in sensor networks for multiple target tracking", in *Distributed Computing in Sensor Systems 5067,* Springer, 2008, pp. 498-509.

[50]. T. S. Fu, A. Ghosh, E. A. Johnson, and B. Krishnamachari, "Energy-efficient deployment strategies in structural health monitoring using wireless sensor networks", in *Structural Control and Health Monitoring*, John Wiley & Sons, 2012, pg. 1-14.

[51]. G. Cevik, M. F. Aksit, and A. Sabanovic, "Piezoelectric wind power harnessing- an overview", in *Proceeding of The 10th International Conference on Sustainable Energy Technologies*, Istanbul, Turkey, Sep 4-7 2011.

[52]. E. Hourdakis and A. G. Nassiopoulou, "A thermoelectric generator using porous Si thermal isolation", in *Sensors 2013 (13)*, pp. 13596-13608.

[53]. D.A. Wang and N.Z. Liu, "A shear mode piezoelectric energy harvester based on a pressurized water flow," in *Sensors and Actuators, A: Physical 167 (2)*, 2011, pp. 449–458.

[54]. M. Yarvis and W. Ye, "Tiered architectures in sensor networks", in *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, edited by M. Ilyas and I. Mahgoub, CRC. Press, Boca Raton, USA, 2005.

[55]. A. Younis and S. Fahmy, "Distributed clustering in ad-hoc sensor networks: a hybrid, energy efficient approach", in *Proceeding of IEEE Infocom 2004*, Hong Kong, March 7-11 2004.

[56]. S. Bandyopadhyay and E. J. Coyle, "An energy efficient hierarchical clustering algorithm for wireless sensor networks", in *Proceeding of IEEE Conference pn Computer Communications*, San Fransisco, USA, March 30 – Apr, 2003, pp. 1713 – 1723.

[57]. R. T. Raj, M. V. Ramesh, and S. Kumar, "Fault tolerance clustering approaches in wireless sensor network for landslide area monitoring", in *Proceeding of 2008 International Conference on Wireless Networks (ICWN 2008)*, Las Vegas, USA, July 14 – 17 2008, pp. 107 – 113.

[58]. C. Y. Wen and W. A. Sethares, "Automatic decentralized clustering wireless sensor networks", in *EURASIP Journal on Wireless Communications and Networking 2005 (5)*, pp.686-697.

[59]. B. Aoun and R. Boutaba, "Clustering in WSN with latency and energy consumption constraints", in *Journal of Network and Systems Management 14 (3)*, September 2006, pp. 415-439.

[60]. B.S. Manoj and R.R. Rao, "Wireless mesh networks: issues and solutions", In *Wireless mesh networking: architectures, protocols, and standards*, edited by Y. Zhang, J.J. Luo, and H.L. Hu. Taylor and Francis Group, LLC. Boca Raton, USA, 2007, pp. 8-11.

[61]. P. Karn, "MACA – a new channel access method for packet radio" in *Proceeding of the ARRL/CRRL Amateur Radio 9^th^ Computer Networking Conference*, September 22 1990, pp.134-140.

[62]. F. Talucci, M. Gerla, and L. Fratta, "MACA-BI (MACA by invitation) – a receiver oriented access protocol for wireless multihop networks, in *Proceeding of IEEE PIMRC 1997*, Helsinki, Finland, 1997, pp.435-439.

[63]. Y. Wang and J. J. Garcia-Luna-Aceves, "A new hybrid channel access scheme for adhoc networks", in *ACM Wireless Networks Journal, Special Issue on Ad Hoc Networking 10 (4)*, 2004.

[64]. T. Sugimoto, N. Komuro, H. Sekiya, S. Sakata, and K. Yagyu, "Maximum throughput analysis for RTS/CTS-used IEEE 802.11 DCF in wireless multi-hop networks", in *Proceeding of International Conference on Computer and Communication Engineering (ICCCE 2010)*, Kuala Lumpur, Malaysia, May 11-13 2010.

[65]. C. Wu and V. Li, "Receiver-initiated busy-tone multiple access in packet radio networks", in *Proceeding of ACM Worksop on Frontiers in Computer Communication Technology (SIGCOMM '87),* Stowe, USA, August 11-13 1987, pp. 336-342.

[66]. J. Deng and Z. Haas, "Dual busy tone multiple access (DBTMA): a new medium access control for packet radio networks", in *Proceeding of IEEE ICUPC 1998,* Oct. 1998, pp. 973-977.

[67]. R. R. Choudhury, X. Yang, R. Ramanathan, and N. H. Vaidya, "Using directional antennas for medium access control in ad hoc networks", in *Proceeding of The 8th Annual International Conference on Mobile Computing and Networking 2002 (Mobicom 2002),* Atlanta, USA, September 23-28 2002, pp. 59-70.

[68]. T. Korakis, G. Jakilari, and L. Tassiulas, "CDR-MAC: a protocol for full exploitation of directional antennas in adhoc wireless networks", in. *IEEE Transactions on Mobile Computing 2007*, pp. 145-155.

[69]. J. Wang, H. Zhai, P. Li, Y. Fang, and D. Wu, "Directional medium access control for ad hoc networks", in *Wireless Networks 15 (8)*, 2009, pp. 1059-1073.

[70]. M. Nilsson, "Directional antennas for wireless sensor networks", in *Proceeding of The 9th Scandinavian Workshop on Wireless Adhoc Networks (Adhoc'09),* Uppsala, Sweden, May 4-5 2009, pp. 1-4.

[71]. G. Giorgetti, A. Cidronali, S. K. Gupta, and G. Manes, "Exploiting low-cost directional antennas in 2.4 GHz IEEE 802.15. 4 wireless sensor networks", in *Proceeding of The 2007 European Conference on Wireless Technologies*, Munich, Germany, October 8-12 2007, pp. 217–220.

[72]. H. S. W. So, J Walrand, and J. Mo, "McMAC: a parallel rendezvous multi-channel MAC protocol", in *Proceeding of Wireless Communication and Networking Conference 2007 (WCNC 2007)*, Hongkong, March 11-15 2007.

[73]. Texas Instruments, "CC2420, 2.4 GH IEEE 802.15.4/ZigBee-ready RF Transceiver", https://ti.com /lit/ds/symlink/cc2420.pdf, accessed on May 12 2017.

[74]. D. G. M. Dang, and C. S. Hong, "H-MMAC: a hybrid multi-channel MAC protocol for wireless ad-hoc network", in *Proceeding of The 3rd IEEE International Workshop on Smart Communications in Network Technologies 2012 (SaCoNet-III),* Ottawa, Canada, June 10-15, 2012, pp. 6489-6493.

[75]. C. Y. Chang, C. H. Kuo, C. Y. Hsiao, and C. C. Chen, "A multi-channel MAC protocol for improving channel utilization in wireless networks", in *Proceeding of The 8th EUROSIM Congress on Modelling and Simulation 2013 (EUROSIM 2013),* Cardiff, UK, Sept. 10-13 2013, pp. 579-584.

[76]. S. Biswas and R. Morris, "Opportunistic routing in multi-hop wireless networks", in *ACM SIGCOMM Computer Communication Review 43(1),* January 2004, pp. 69-74.

[77]. K. Zeng, W. Lou, J. Yang, and D. R. Brown III, "On throughput efficiency of geographic opportunistic routing in multihop wireless networks", in *Mobile Network Applications 12, 2007,* pp. 347-357.

[78]. J. Du, H. Liu, and P, Chen, "OMR: an opportunistic multi-path reliable routing protocol in wireless sensor networks", in *Proceeding of International Conference on Parallel Processing Workshops (ICPPW 2007),* 2007.

[79]. M. Mafuta, M. Zennaro, A. Bagula, G. Ault, H. Gombachika, and T. Chadza, "Successful deployment of a wireless sensor network for precision agriculture in Malawi", in *International Journal of Distributed Sensor Network 2013,* 2013, pp. 3-13.

[80]. A. Grilo, H. Sarmento, M. Nunes, J. Goncalves, P. Pereira, A. Casaca, and C. Fortunato, "A wireless sensors suite for smart grid applications", in *International Workshop of Information Technology for Energy,* 2012, pp. 11-20.

[81]. V. C. Gungor and G. P. Haneke, "Industrial wireless sensor networks: challenges, design principles, and technical approaches", in *IEEE Transsactions on Industrial Electronics 56 (10),* 2009, pp. 4258-4265.

[82]. Y. Yao and J. Gehrke, "Query processing for sensor networks", in *Proceeding of 2003 Conference on Innovative Data Systems Research (CIDR 2003),* Asilomar, USA, January 5-8 2003.

[83]. R. Steighmann and J. Endresen, "*Introduction to WISA, wireless interface for sensors and actuators*", white paper, ABB, 2006.

[84]. M. A. Yigitel, O. D. Incel, and C. Ersoy, "QoS-aware MAC protocols for wireless sensor networks: a survey", in *Computer Networks 55*, 2011, pp. 1982-2004.

[85]. C. T. Calafate, P. Manzoni, and M. P. Malumbres, "Assessing the effectiveness of IEEE 802.11e in multi-hop mobile network environments", in *Proceeding of The IEEE Computer Society's 12th Annual International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunications Systems (MASCOTS '04)*, 2004.

[86]. K. L. Hua and R. G. Cheng, *"Performance evaluation of 802.11e over multihop wifi mesh networks"*, https://www.researchgate.net/publication/254344472_Performance_Evaluation_of_80211e_over_Multihop_WiFi_Mesh_Networks, accessed on June 10 2017.

[87]. Y. Shimoyamada, K. Sanada, N. Komuro, and H. Sekiya, "End-to-end throughput analysis for IEEE 802.11e EDCA string-topology wireless multi-hop networks", in *IEICE Nonlinear Theory and Its Applications 6(3)*, 2015, pp. 410-432.

Every reasonable effort has been made to acknowledge the owners of copyright material.
I would be pleased to hear from any copyright owner who has been omitted or incorrectly acknowledged.