

ENSC 835: COMMUNICATION NETWORKS

SPRING 2011

PRESENTATION OF PERFORMANCE EVALUATION OF KEY 802.11 MAC PROTOCOLS

Yitao Wu

Student ID, 301127569

Email Address, yitaow@sfu.ca

Biao Li

Student ID, 301154307

Email Address, biaol@sfu.ca

Team 8

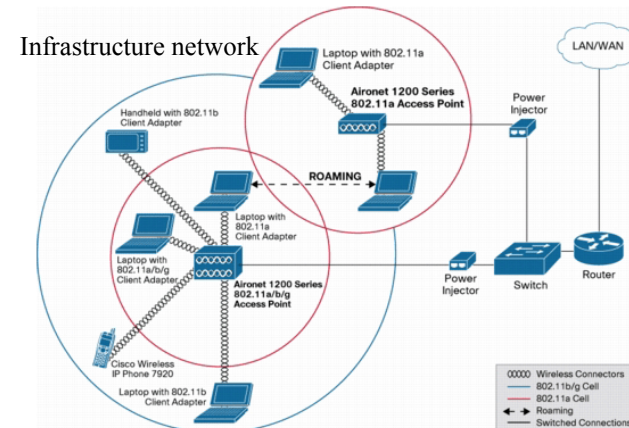
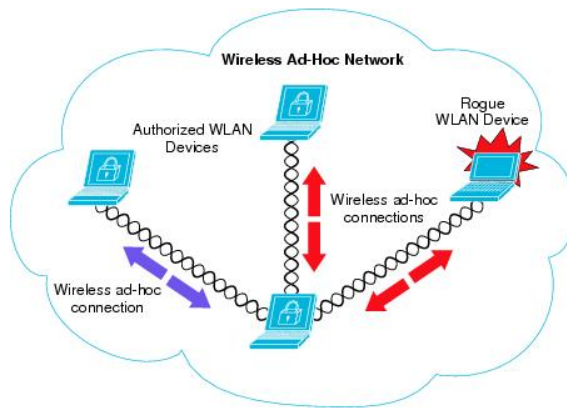
Supervised by Professor Ljiljana Traikovic

<http://www.sfu.ca/~yitaow/ensc835/index.html>

<http://www.sfu.ca/~biaol/ensc835/index.html>

Introduction to IEEE 802.11

- IEEE 802.11 is a set of standards carrying out wireless local area network (WLAN) computer communication in the 2.4, 3.6 and 5 GHz frequency bands. They are created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802).
- The nodes in a wireless domain can work as an ad hoc network or infrastructure network.
- Advantages of IEEE802.11 wireless LAN technologies - wire-free, increasingly popular: hotspots (airport, cafeteria).
- Difficulties to implement IEEE 802.11
 - **Error-prone channel.** Unlike the fibre or coax channel of the Ethernet, the air channel of WLAN (IEEE 802.11) is a fading channel with interference. The bit error is much higher than the Ethernet.
 - **Hidden node problem.** When a node is visible from some wireless nodes, but not from other nodes.



MAC Layer of IEEE 802.11

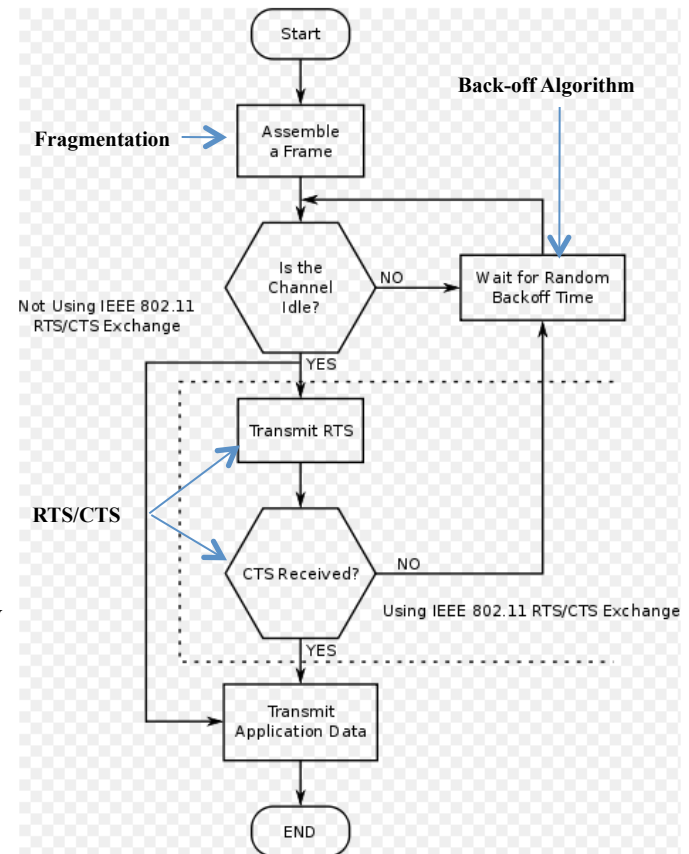
- The IEEE 802.11 WLAN protocol covers two layers (the Data Link Layer and Physical Layer) and compliant to the OSI model. The 802.11 Standard currently defines a single MAC which interacts with three PHYs (FSS, DS, and IR).

802.2			Data Link Layer
802.11 MAC			
FH	DS	IR	PHY Layer

- Main Protocol of MAC - Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). Unlike CSMA/CD (Carrier Sense Multiple Access/Collision Detect) implemented in the Ethernet which deals with transmissions after a collision has occurred, CSMA/CA acts to prevent collisions before they happen.
- What is the difference between CSMA/CD and CSMA/CA and Why** - In CSMA/CD it detects that a collision takes place by monitor the physical channel and resend the frame that was send. On a wireless network, the signal received from other nodes is very weak compared to its sending signal. Collision detection is not possible when data sending is in progress. so CSMA/CA was deployed.

Key Features of MAC Layer

- **RTS/CTS (Request to Send/Clear to Send)**
 - RTS/CTS handshake before sending packets, similar to TCP connection
 - To solve the problem of Hidden Node
 - Optional feature
- **Fragmentation**
 - To divide the large packets smaller to avoid retransmitting large packets in the presence of RF interference or in a fading wireless environment.
 - Optional feature
- **Back-off Algorithm**
 - A algorithm to let node wait for a while before delivery when collision occurs in busy time.
 - 802.11 mainly use DCF. There is no arbiter.
 - Each node has to cooperate with each other to use the channel fairly



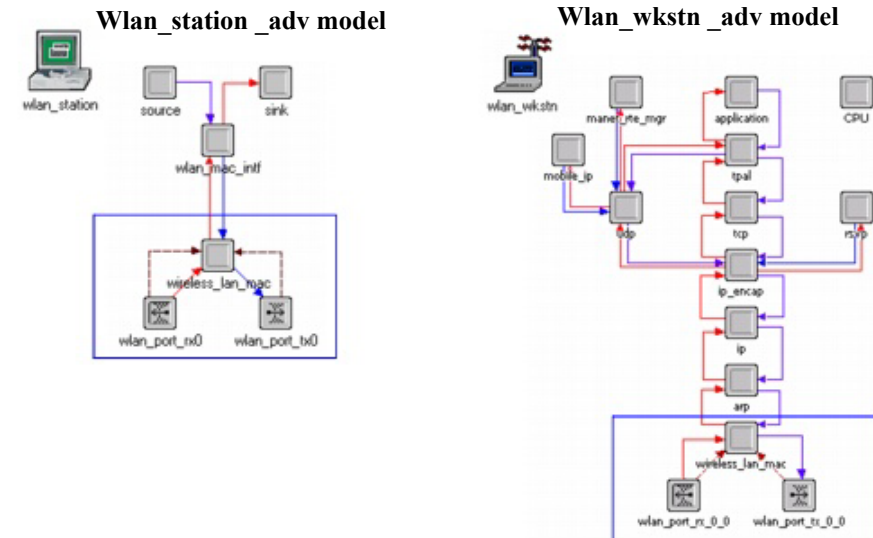
OPNET and Simulation

- **OPNET and Wireless Model**

- OPNET is the industry's leading network simulation tool for TCP/IP wired and wireless network.
- The OPNET WLAN model provide high-fidelity modeling, simulation, and analysis of wireless LAN networks, including the RF environment, interference, transmitter/receiver characteristics, and full protocol stack, including MAC, routing, higher layer protocols and applications.
- A full set of wireless nodes have been provided in the node model category

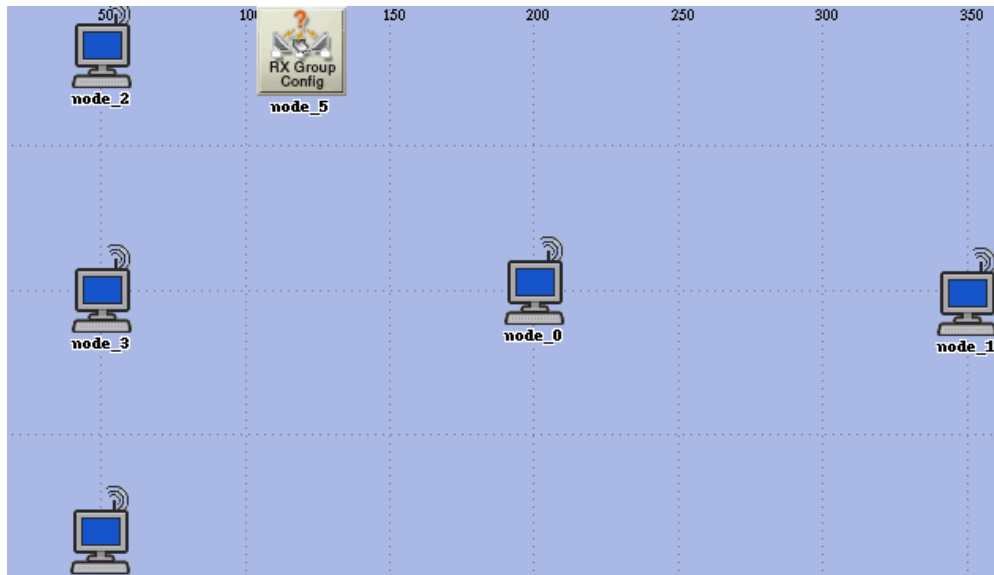
- **Wlan_station_adv Model**

- This project focus on the evaluation of the feature of MAC layer protocol.
- Wlan_station_adv, which has the WLAN MAC without a higher-layer stack (source and sink models to simulate higher layers) is more suitable for our study compared to wlan_wkstn_adv model.
- Avoid the interference from upper level protocol

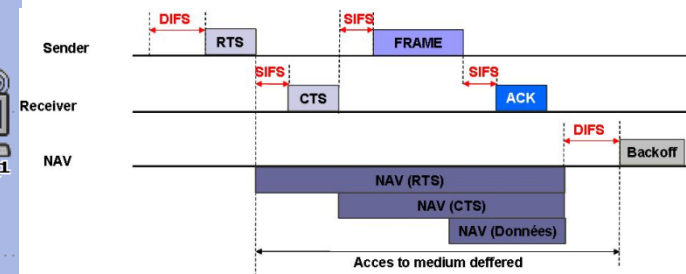


Implementation – RTS/CTS Evaluation

- **Network topology** - A small and simple 5 nodes wireless LAN network is simulated. The Node 0 in the center acts as AP, receiving data from the Nodes 1-4. Node 1 acts as Hidden Node to the node 2-4.
- **Hidden Node** - The tool “Rx Group Config” is introduced to hide the Node 1 from node 2-4.
- **Network configuration** - Distance Threshold of “Rx Group Config” was defined to group receiver of nodes 0-4. Node 0-1 belong one group, node 0, 2-4 is in another group

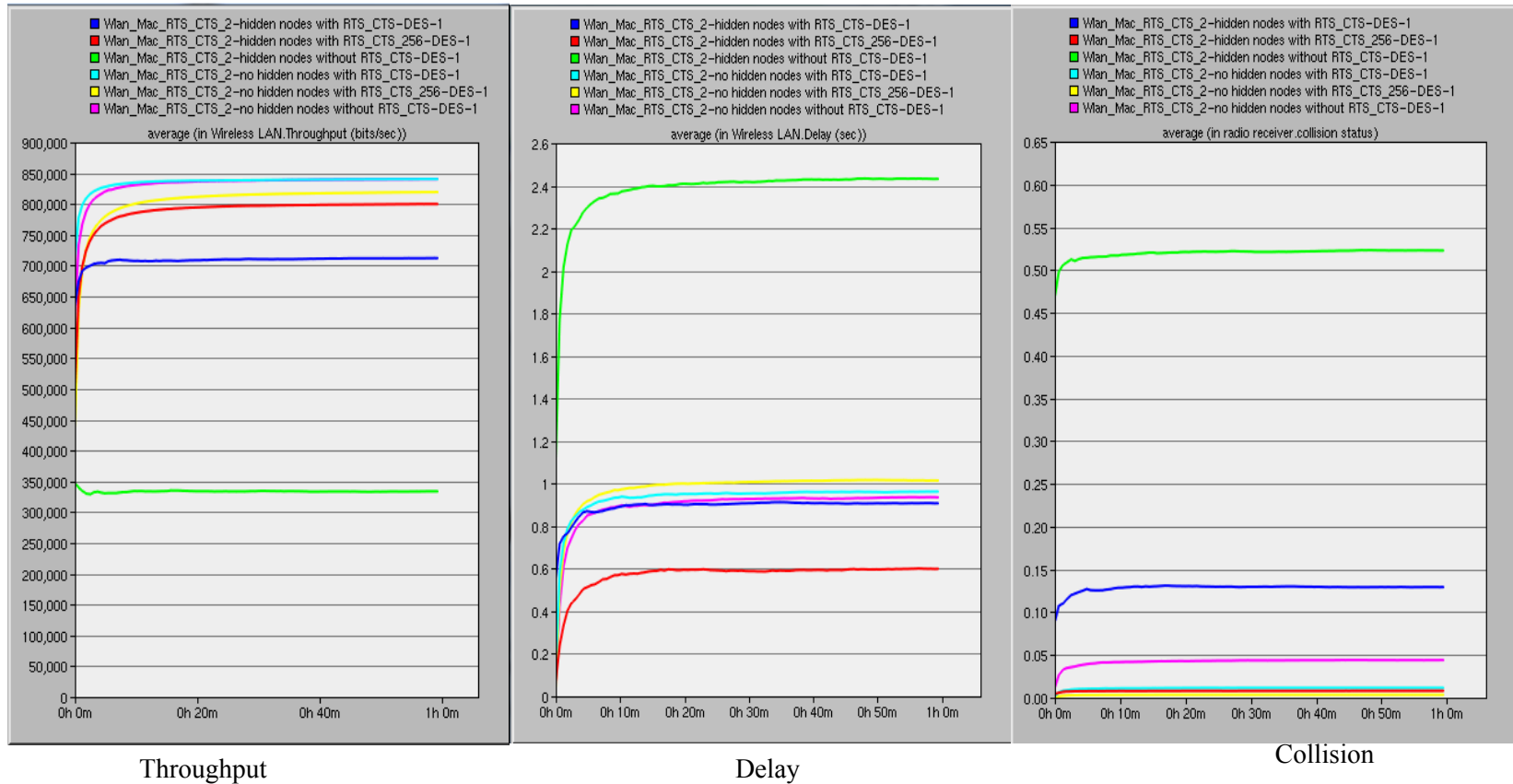


RTS/CTS Flow Chart



Results – RTS/CTS Evaluation

- Simulation time – 60minutes
- Collect simulation statistics – Throughput, delay, collision.



Analysis – RTS/CTS Evaluation

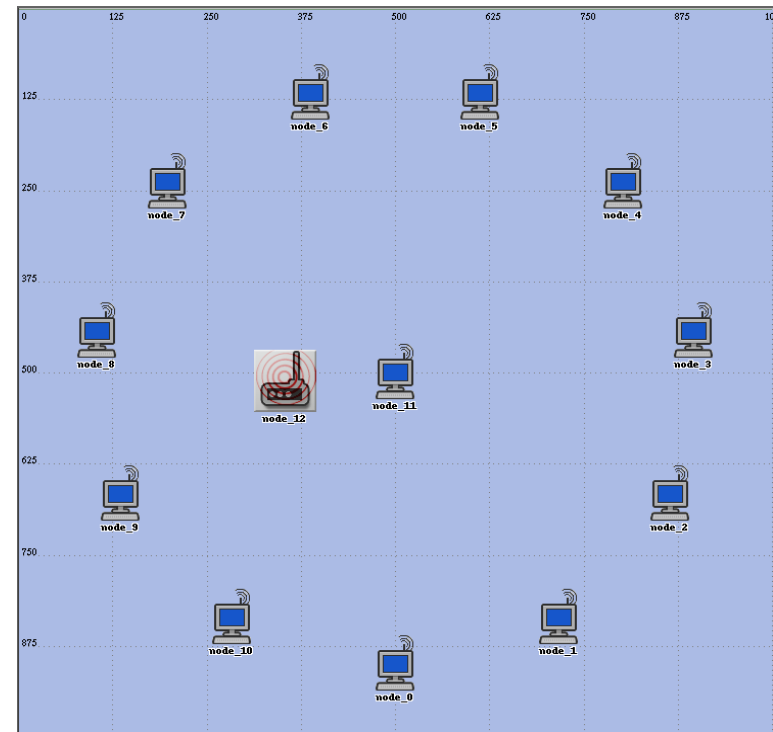
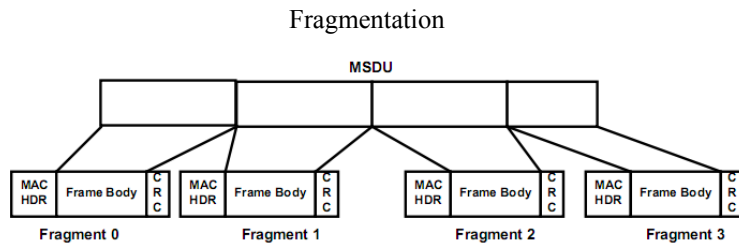
- If no Hidden Nodes the AP has highest throughput. The option of RTS/CTS on or off does not affect the performance too much.
- When the Hidden Node presents in the network and no RTS/CTS, the network performance dramatically drop down, lowest throughput, longest delay and most collision.
- Turning the RTS/CTS on can improve the performance of the network in which hidden nodes present.
- Reduce the threshold of the RTS/CTS will further improve the throughput and reduce delay when hidden nodes present.
- Although the throughput is increased when we reduced the threshold, it is still not better than no hidden nodes scenario with same parameters.
- RTS/CTS can affect collision directly, but it affect other performance indirectly. Reducing collision can not guarantee to improve other performance.

Implementation – Fragmentation Evaluation

- **Network topology** – 11 nodes network. Node 11 in the center act as receiving only AP. Nodes 1-10 work as sending only nodes.
- **Jammer Node** – Jammer Node is introduced in the network to simulate the interference.
- **Scenarios** – 8 scenarios have been studied in this project.

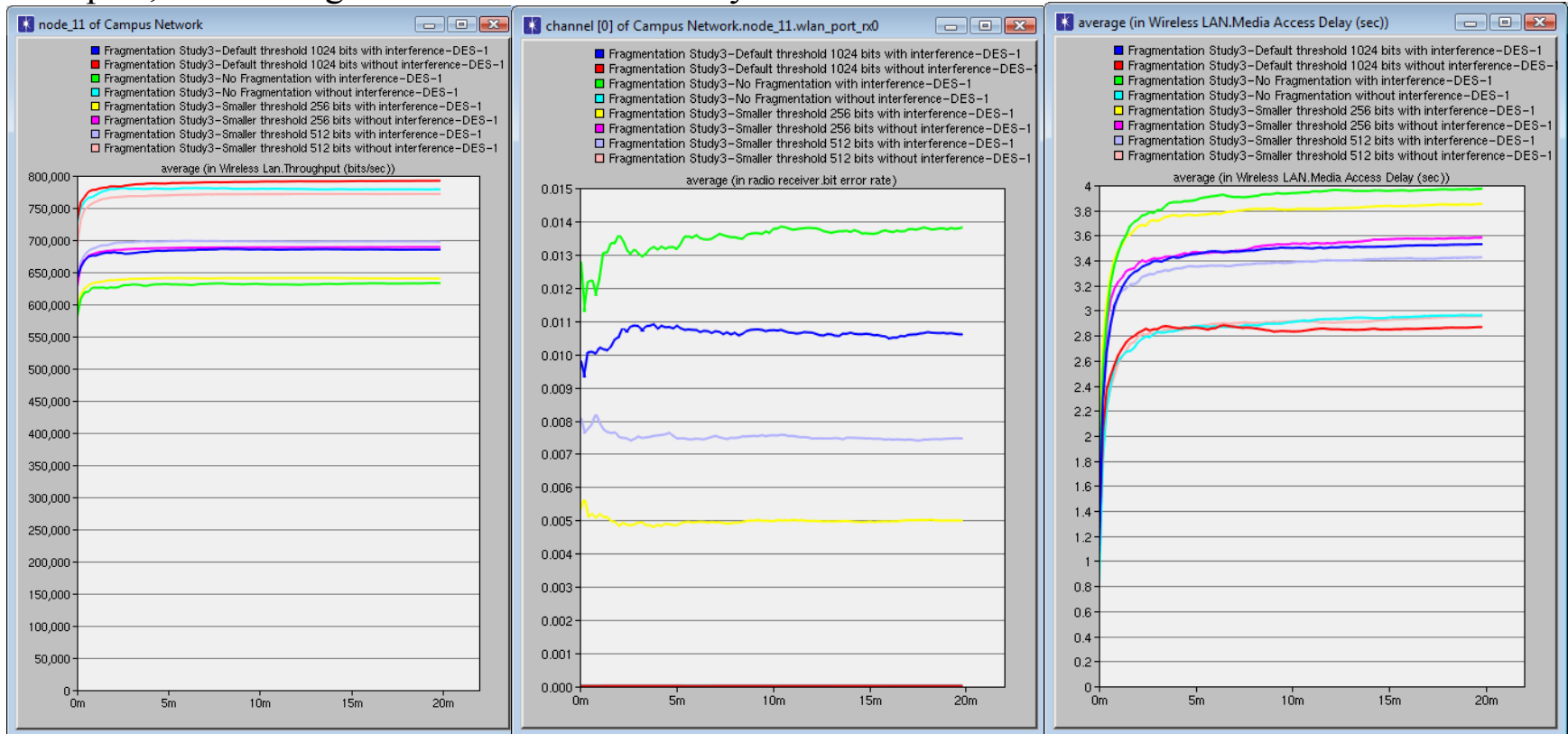
Scenarios:

1. No Fragmentation without interference.
2. No Fragmentation with interference.
3. Default threshold 1024 bytes without interference.
4. Default threshold 1024 bytes with interference.
5. Threshold 512 bytes without interference.
6. Threshold 512 bytes with interference.
7. Threshold 256 bytes without interference.
8. Threshold 256 bytes with interference.



Results – Fragmentation Evaluation

- Simulation time – 20minutes
- Collect simulation statistics – Throughput of Node 11, The bit error in the Node 11's receiver port, the sending nodes media access delay.



Throughput of Node 11

Bit error rate of the receiver port of Node 11

Media access Delay of the sending Nodes

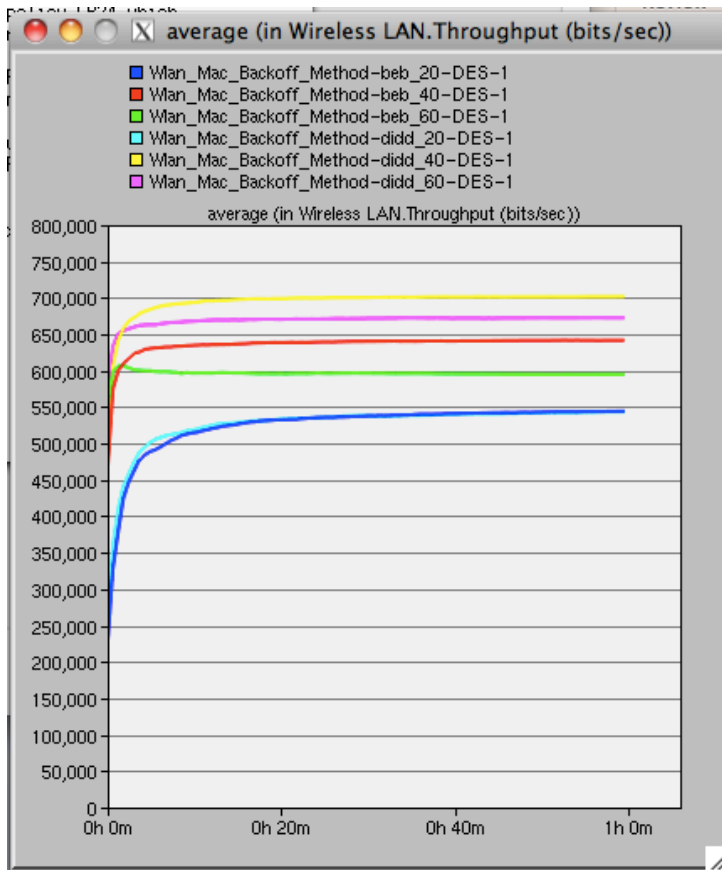
Analysis – Fragmentation Evaluation

- **Throughput** – In the ideal wireless environment, the default 1024 bytes threshold scenario has the highest throughput. When the threshold reduce the throughput reduce. However when we increase the threshold or leave the Fragmentation feature off, the throughput decrease. In the real wireless environment with fading and interference, the 512 bytes threshold scenario has the highest throughput. The no Fragmentation scenario has the worst throughput. The Fragmentation feature works very well in the error-prone channel.
- **Bit error in the receiver of Node 11** – As we can expect, in the ideal wireless environment there is no bit error. When the interference presents in the network, the bigger the packet size the higher the bit error rate.
- **Media Access Delay** – In the ideal wireless environment, the threshold 1024 bytes scenario has least delay. When the interference presents in the network, the bigger the packet size the more delay introduced by the retransmission. However if the threshold is too small, the overhead will increase the delay.

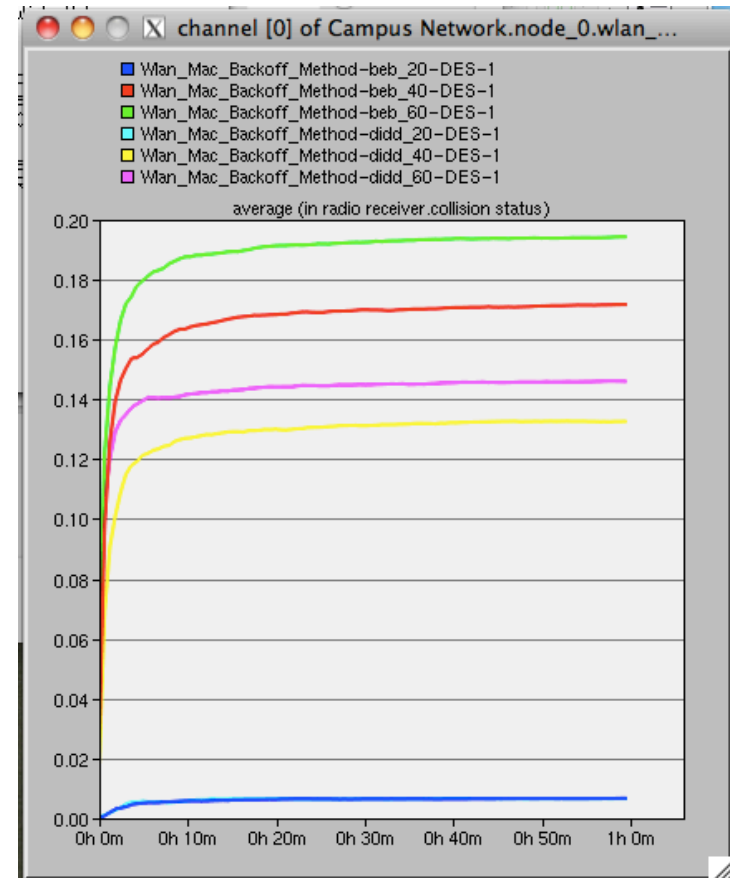
Implementation – Backoff Algorithm

- **802.11 original algorithm: BEB.**
 - Double congestion window when collision
 - Reset congestion window when successfully deliver.
 - Drawback:
 - Unfair
 - Not reflect past situation of network
- **Chatzimisios' new algorithm: DIDD.**
 - Double congestion window when collision
 - Halve congestion window when successfully deliver.
 - Goodness
 - Simple
 - More fairness
 - Reduce collision possibility after shrink congestion window
- **20, 40 and 60 wireless nodes build ad hoc network.**
 - Use same parameter
 - Generate different traffic

Results – Backoff Algorithm



Average Throughput



Collision

Analysis – Backoff Algorithm

- In scenario of 20 nodes, the traffic is low and collision is light, the two algorithms have no difference. Their lines are close to each other
- In scenario of 40 and 60 nodes, the traffic is very high and collision is heavy, the DIDD get more throughput and low collision.
- From 20 nodes to 40 nodes, the performance is increased. The free bandwidth is used by new nodes. From 40 to 60 nodes, the performance is dropped down. Because there is no free bandwidth, and more collisions occur.
- Because DIDD halves congestion window, it encounters less collision in heavy traffic.

Conclusion and Discussion

- 802.11 WLAN is a distribution system
- CSMA/CA provides a contention free media access mechanism.
 - CSMA/CD is a collision detect mechanism. It works very well in the error-free or low error environment. However it does not work well in the error-prone wireless environment. The sending node can not sense the collision when the sending is in progress.
 - Carrier avoid mechanism is developed to suit the characteristic of the wireless channel.
 - Some key features in this suite have been evaluated in our projects.
- RTS/CTS
 - Hidden node is a common phenomena, because RF is a error-prone channel and it is easy to be weaken .
 - RTS/CTS let other nodes find hidden node indirectly
 - CSMA/CA provides the mechanism of listening channel before sending to avoid collision. RTS/CTS goes further. It reduces the cost of collision.
 - The cost of using RTS/CTS is very small. It can be ignored in some situation but should be concerned in others.
- Fragmentation
 - **Reliability, Throughput and Media Access Delay-** The use of fragmentation can increase the reliability of frame transmissions by sending smaller frames. Less collisions and smaller packet retransmission means higher throughput and lower delay.

Conclusion and Discussion (Cont')

- **On or Off** – The Fragmentation is also a optional feature. This feature does not improve performance in an ideal wireless channel (no error or low error rate). It works effectively in the fading or interference wireless environment. The collisions (less than 5 percent) is a parameter to be monitored to decide if the Fragmentation should be set on.
- **Threshold size** – The threshold of the Fragmentation should set to a reasonable value. Too small value will dramatically increase the overhead on the network, reducing throughput.
- **Back-off algorithm**
 - BEB is simple and useful in most situation
 - Because of characteristic of DCF, each node has no overview of whole network. So it is not reasonable to reset congestion window according one time of successful deliver.
 - DIDD resolve some problem of BEB. It halves congestion to avoid the next collision. The collision number is reduced, the performance is increased. But it only works well at heavy traffic.
 - DIDD only change reset function of BEB. It is easy to implement.
 - More back-off algorithms is being designed. They use more information of current network to decide congestion window.
- 802.11 WLAN is a group of successful technology , but it is still under changing for accommodating new technology and user requirement.

Reference:

- IEEE "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications" 2005
- Crow, B.P. , Widjaja, I. , Kim, L.G. ,Sakai, P.T. . IEEE 802.11 Wireless Local Area Networks. IEEE Communications Magazine, Vol. 35 Issue 9, Sep 1997, pp.116-126
- Manshaei, M.H. , Cantieni, G.R. , Barakat, C. , Turletti, T.. Performance analysis of the IEEE 802.11 MAC and physical layer protocol. World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. Sixth IEEE International Symposium on a Digital Object Identifier: 10.1109/WOWMOM.2005.76
- Matthew S. Gast. 802.11 Wireless Networks: The Definitive Guide, O'Reilly Press. Chapter 2,Chapter 3, Chapter 4, Page 12-113
- Wu HaiToa, LIN Yu, ChENG ShiDuan, PENG Yong, Long KePing. IEEE 802.11 Distributed Coordination Function: Enhancement and Analysis. J. Comput. Sci. & Technol, Sept. 2003, Vol.18, No. 5, pp.607-614
- P. Chatzimisios, V. Vitsas, A. C. Boucouvalas, M. Tsoulfa. Achieving performance enhancement in IEEE 802.11 WLANS by using the DIDD backoff mechanism. Int. J. Commun. Syst. 2007; 20:23-41
- OPNET documentation: "Model Library: Wireless Lan" and "Modules: Wireless"
- OPNET Wireless module: node module "wlan_station_adv", process module "wlan_dispatch", "wlan_mac".