The Case for Heterogeneous Wireless MACs

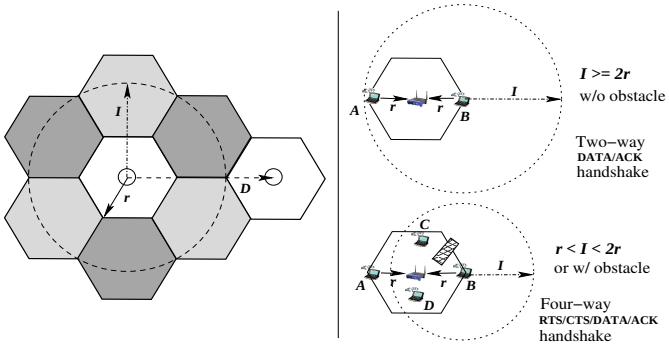
Chun-cheng Chen and Haiyun Luo
Dept. of Computer Science, UIUC
{chen35,haiyun}@cs.uiuc.edu

ABSTRACT

Current 802.11[1] WLANs rely on the 802.11 MAC (medium access control) and careful channel assignment to resolve intra- and inter-BSS (basic service set) interferences respectively. However, because wireless transmissions interfere with each other in a range that is larger than the communication range and because there is only a very limited number of orthogonal channels, an 802.11 client contends with not only the clients located in the same BSS, but also the clients located in other BSS's operating on the same or overlapping channels. Consequently, the well-known hidden/exposed terminal problem emerges and causes serious packet losses and flow starvation. In this paper, we show that the hidden/exposed terminal problem is the result of *context-dependent* channel status assessment, which is often *incomplete* at an 802.11 transceiver and *inconsistent* at different contending transceivers. A MAC protocol that is *homogeneous* across the contending transceivers, for the good reason of inter-operability, cannot produce accurate channel status assessment for *all* of them, and is therefore ineffective in dealing with the hidden/exposed terminal problem. We then explore a simple self-learning approach that leads to structurally *heterogeneous* MAC protocol designs. These MAC protocols are tailored to the specific context of the sender and the receiver to compensate their context-dependent channel status assessment. A single set of signaling messages are defined for inter-operability among heterogeneous MAC protocols and backward compatibility with the legacy 802.11 MAC. The preliminary simulation results show that heterogeneous MAC protocols handle intra-/inter-BSS interferences induced hidden/exposed problem very well. Our method opens new space for wireless network protocol designs, and can potentially be applied to solve other open network problems.

1. 802.11 INTERFERENCE MITIGATION

The current deployment of 802.11 WLANs relies on channel assignment to resolve inter-BSS (basic service set) interferences. To this end, a minimum number of $N \geq \frac{1}{3}\left(\frac{D}{r}\right)^2$ orthogonal channels are necessary to cover a two-dimensional space, as shown in Figure 1 (a). Note that r is the *communication range* in which the signal-to-noise (SNR) is high enough for a receiver to decode the wireless transmissions, and D is the minimum distance between two base stations that reuse the same channel. Further beyond the communication range from the sender is the *blocking range*, denoted as I in Figure 1 (a), in which a receiver can decode[2] neither the transmitted frame due to low SNR, nor the frames from any other transmitter within communication range due to high interferences (low signal-to-interference-noise ratio (SINR)). Considering wireless clients located around the boundaries of the BSS's we can see that inter-BSS interferences can be resolved only if $D > I+2r$, or $N > \frac{1}{3}\left(I/r+2\right)^2$.



(a) Optimal channel assignment for inter−BSS interference mitigation

(b) 802.11 clear channel assessment for intra−BSS contention mitigation

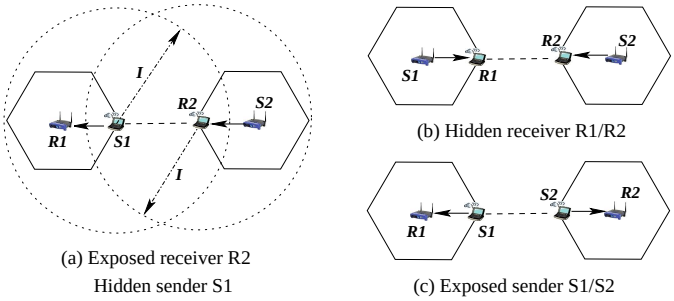
Figure 1: Inter-/intra-BSS interference mitigation in an 802.11 WLAN.

Assuming that the channel assignment eliminates inter-BSS interferences, 802.11 MAC (medium access control) resolves intra-BSS interferences quite well with the mandatory 802.11 CCA (clear channel assessment) and the optional four-way (RTS/CTS/DATA/ACK) handshake, as shown in Figure 1 (b). 802.11 CCA dictates that every 802.11 transceiver maintains a built-in CS (carrier sense) threshold, which matches the lowest RSS (received signal strength) of a transmission within the blocking range. If the RSS (received signal strength) is measured above the CS threshold, a "channel busy" is reported by the CCA and the node is refrained from accessing the channel. As long as the blocking range is longer than twice the communication range (i.e., $I > 2r$) and there is no obstacle blocking signal propagation between two clients, every on-going DATA transmission will be sensed (i.e., CCA reporting channel busy) at all other clients in the BSS. Therefore no intra-BSS interferences will be possible.

Otherwise, e.g., when $r < I < 2r$ or when obstacles exist, a client located on the other side of the BSS (e.g., client A in Figure 1 (b) bottom) or being blocked by the

[1]We abuse "802.11" to denote the IEEE 802.11 family.

[2]Decode with an error rate lower than the targeted threshold.



(a) Exposed receiver R2 Hidden sender S1

(b) Hidden receiver R1/R2

(c) Exposed sender S1/S2

Figure 2: Hidden/exposed terminal problem in 802.11 WLANs due to inter-BSS interferences.

obstacle (e.g., client C) will not be aware of and therefore may interrupt an on-going DATA transmission from another client (e.g., client B) to the access point. To deal with these scenarios 802.11 defines an optional four-way handshake with short RTS/CTS (request-to-send/clear-to-send) messages exchanged between client B and the access point before DATA/ACK. Since all clients in the BSS, including clients A and C, must be within the communication range from the access point, they will receive the CTS and be refrained from accessing the channel until the access point receives the DATA. However, 802.11 standard does not specify how a BSS chooses to enable four-way handshake. Since the RTS/CTS incur a minimum 37% and 29% overhead on throughput for 11Mbps 802.11b and 54Mbps 802.11a/g respectively[3], the optional four-way handshake is usually disabled by default and enabled manually in very rare scenarios.

2. HIDDEN/EXPOSED TERMINAL

The limited number of orthogonal channels[4] defined in 802.11, e.g., 3 for 802.11b/g and 12 for 802.11a in U.S., are usually not enough to eliminate the inter-BSS interferences. The three orthogonal channels in 802.11b/g could be barely enough only if the blocking range is equal to the communication range, i.e., $I = r$, and the channel assignment is network-wide optimal. The former is not true with any real 802.11 wireless transceivers, while the later usually ends up as good will only in reality due to the widespread, autonomous installations of 802.11 home networks and hotspots. Recently published data on metropolitan area 802.11 coverage [3, 2, 5] show that more than 40% of the access points are operating on channel 6. In Boston, a maximum number of 85 access points were detected in blocking range of each other [5, 2], which leads to at least 28 interfering BSS's given that the majority of the access points are 802.11b/g.

As a result of the inter-BSS interferences, the well-known hidden/exposed terminal problem [9], an open problem that has been haunting in the research community for more than a decade, emerges in 802.11 WLANs. We illustrate the problem with Figure 2[5], where two BSS's sharing the same (or overlapping) channel are analyzed.

Figure 2 (a) shows the **exposed receiver** and **hidden sender** problem. With 802.11's default two-way handshake, sender S1 sends out the DATA and receiver R1 replies with an ACK. However, the sender S2, located outside the blocking range of S1, is not aware of the on-going transmission between S1 and R1. Therefore, S2 may send out DATA to R2, which is blocked by (or exposed in) the transmission of S1. Note that 802.11's optional four-way handshake with RTS/CTS (request-to-send/clear-to-send) will not help resolve the exposed receiver problem, since sender S2 cannot decode the RTS from S1 or CTS from R1, and therefore cannot correctly assess the channel status at receiver R2. Similarly, if S2 is transmitting to receiver R2, sender S1 becomes a hidden sender. Again since S1 is not aware of the on-going transmission between S2 and R2, it may transmit DATA and corrupt the on-going reception at R2. Note that in this case 802.11 four-way handshake potentially helps if S1 and R2 are located within communication range, since S1 will receive R2's CTS message and wait until the transmission from S2 to R2 finishes. However, our evaluation shows that the four-way handshake helps only when the offered load is light and the hidden sender problem is not serious. The reason is that receiver R2's CTS is triggered by non-interfered reception of S2's RTS. That is, sender S2 has to send out the RTS when sender S1 is idle. Under heavy load S1 is idle only in inter-frame backoff, and 802.11's CCA (clear channel assessment) at S2 provides no useful information for S2 to catch the fleeting chance.

Figure 2 (b) shows the **hidden receiver** problem, where the receiver that receives the DATA packet first will send out the ACK and corrupt the reception at the other receiver. In this scenario 802.11 four-way handshake will, again, help only if R1 and R2 are located within communication range, where the CTS will exclude the situation where both receivers receive DATA at the same time. Finally the **exposed sender** problem, as shown in Figure 2 (c), is the only problem that is handled well by 802.11's CCA. Since both senders are within at least the blocking range from each other, one sender that attempts to access the channel after the other will assess the channel busy. The backoff timer of the sender will then freeze until the on-going transmission finishes and CCA reports channel idle again. Senders S1 and S2 will therefore compete effectively in terms of low packet loss ratio and fairly over both short-term and long-term time intervals.

3. RELATED WORK

Wireless medium access control can be either contention based or schedule based. Contention based schemes are usually preferred in data networks because they achieve higher statistical multiplexing gain, are easier to implement, and are robust to synchronization errors. Collisions have to be resolved in contention based medium access control.

IEEE 802.11 [12] medium access control, predominantly Distributed Coordination Function (DCF), is probably the most popular CSMA/CA MAC. 802.11 was designed for infrastructure mode, where nodes in a BSS can be *at most two hops* away from each other and *communicate only with*

[3]Note that although RTS/CTS sizes are small, there is a constant physical layer overhead for each transmitted frame.
[4]Note that dividing available wireless communication resources into many orthogonal channels will not serve *bursty* data traffic well [7, 13].
[5]We use circle to represent the communication/blocking range. However, we do not assume circular communication/blocking area in our design, and it could be of any dynamic shape in reality.

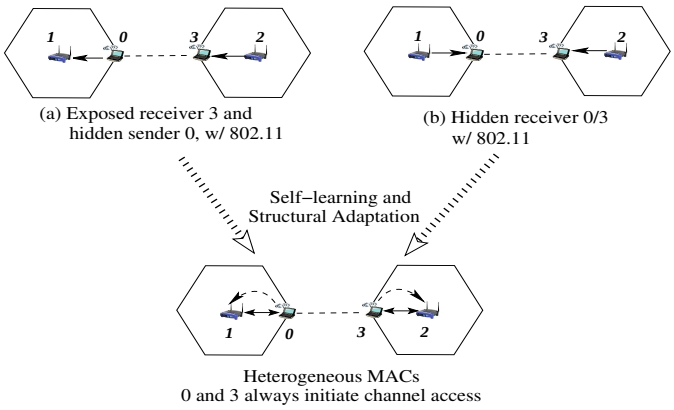


Figure 3: Heterogeneous MACs for hidden/exposed terminal problem

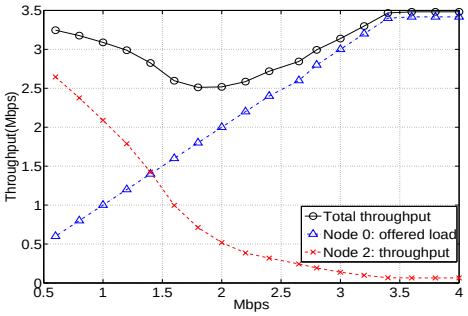


Figure 4: Throughput of two flows in Figure 3(a) with homogeneous 802.11 MAC

the centralized access point. MACAW [9] and FAMA [11] are early proposals on CSMA/CA wireless MAC. They handle hidden/exposed sender problem better than 802.11, but leave the hidden/exposed receiver problem open.

BAPU [8] addresses the hidden/exposed receiver problem, but it requires two channels and dedicates one channel for signaling. Recently several multi-channel variations of 802.11 medium access control are also proposed, e.g., SSCH [6] and MMAC [14], but their goal is to increase network capacity, not to handle hidden/exposed receiver. Moreover, multiple unlicensed 802.11 channels are not always available, e.g., in Japan.

Optimal MAC carrier sense threshold has been studied to maximize the channel reuse [17, 16]. These analysis, however, do not help address hidden/exposed receiver problem and unfair channel access. As we analyzed in Section 1, the hidden/exposed terminal problem exists as long as the number of orthogonal channel is insufficient or the channel assignment is not optimal, no matter how large the blocking area is configured to be.

The receiver-initiated MAC [15] is relevant to our design in that in certain context it is the receiver that initiates the channel access. It solves the literal hidden/exposed "receiver" problem. However, the hidden/exposed sender problem, which is addressed well by 802.11 sender initiated MAC, emerges since a hidden/exposed sender may not be able to respond to the receiver's poll. Our design instead makes the MAC protocol structurally heterogeneous, adaptive based on the perceived collisions and packet loss, and addresses the above dilemma well.

The fairness problem has been studied in 802.11 QoS provisioning. For example, the minimum and maximum backoff counters, the binary backoff algorithm, and the length of inter-frame space can be manipulated to differentiate the throughputs of different packet flows (see [10, 4] and IEEE 802.11e [1] for a summary). However, they all target at a single BSS and assume that the inter-BSS interferences do not exist.

4. HETEROGENEOUS WIRELESS MAC

The fundamental challenges of the hidden/exposed terminal problem are that due to inter-BSS interferences, the channel status assessment at a sender is often *incomplete* in that it does not have an accurate estimate of the channel status at the receiver at packet-level time granularity, while the channel status assessments at multiple competing senders are often *inconsistent* depending on the specific contexts of all involving senders and receivers. We elaborate these observations in the scenario of the exposed receiver and hidden sender, as shown in Figure 3 scenario (a). Sender 0 and receiver 3 are within communication range of each other, and therefore, have complete status of the two competing flows. However, channel access for flow 2→3 is controlled by sender 2, whose channel status assessment is inconsistent with that of sender 0 and incomplete since it is not aware of the status of the competing flow 0→1. Figure 4 shows the simulated throughput of the two flows. Although flow 2→3 is always backlogged throughout the simulation, sender 0 gradually dominates the channel as its offered load increases until flow 2→3 is starved.

Table 1 summarizes the causes and consequences of the hidden/exposed terminal problem. From the table we conclude that ***incomplete* channel status assessment leads to high packet losses while *inconsistent* channel status assessments lead to unfair channel sharing.** Our goals, therefore, are to achieve complete and consistent channel status assessment in an 802.11 WLAN for high channel utilization (i.e., low packet loss ratio) and predictable flow performance (i.e., fair channel sharing).

Our key idea is very simple: **context-dependent channel status assessment can be compensated with context-dependent, heterogeneous MAC protocols**. By context-dependent MAC protocols we mean not only the existing practice of on-line parameter adjustments, but also *protocol structure adaptation*. Targeting the hidden/exposed terminal problem caused by 802.11's context-dependent clear channel assessment, we consider two dimensions of the MAC protocol design space: the adaptation between two-way and four-way handshakes for intra-BSS interference mitigation, and the adaptation between sender- and receiver-initiated channel access for inter-BSS interference mitigation. Note that we do not claim novelty for any of these mechanisms. Instead, we propose strategies for a sender-receiver pair to customize their MAC protocol on-line to adapt to the local *dynamics* of node, traffic, and interference distributions.

4.1 Intra-BSS interference mitigation

Heterogeneous wireless MAC design for intra-BSS interference mitigation can be illustrated using Figure 1 (b) bot-

Problem	Channel Status Assessment	Packet Loss	Fairness	Four-way Handshake
Exposed receiver Hidden sender	Incomplete and Inconsistent	High	Low	Improve fairness under medium load, ineffective under heavy load
Hidden receiver	Incomplete and Consistent	High	High	Reduce packet loss
Exposed sender	Complete and Consistent	Low	High	Not useful in any scenario

Table 1: Incomplete and inconsistent channel status assessment at the sender leads to hidden/exposed terminal problem in 802.11 WLANs.

tom. In that example four-way handshake with RTS/CTS should be enabled for packet transmissions from client C to the access point, since neither client B nor client A can sense the transmission and may interrupt the reception at the access point. For similar reasons four-way handshake should be applied for transmissions from either client B or client A to the access point. On the other hand, when client D is transmitting to the access point two-way handshake should be applied, since all other clients in the BSS will sense the channel busy. RTS/CTS will only bring in extra overhead on throughput for flow D→AP (access point). Therefore, if a client can learn whether or not there exists another active client who may not be able to detect his transmission signal, the client can decide if an RTS should be transmitted before sending the DATA.

It turns out that, for any client determining if it can detect DATA transmissions from any other clients is relatively easier than judging if his own transmission can be detected by all other clients. Under the assumption that the channel is symmetric between two clients these two scenarios are equivalent. Therefore, if a client does not sense the channel busy, for the duration approximate to one packet transmission time, before receiving an ACK message from the access point destined for other client, the client should turn on four-way handshake between itself and the access point. However, if the channel is asymmetric, the client should wait until it hears from at least one hidden client, with the explicit feedback relayed by the access point, before the client enables four-way handshake. If the network is extremely dynamic the overhead of the relayed feedback could be large.

Note that we do not have to go through above complexity if we can simply designate the access point to always initiate the channel access, regardless of the flow directions[6]. However, since it is located in the middle of a BSS, the access point will usually be in the worse position in assessing interferences coming from other BSS's compared with the involving client. We therefore adapt between sender- and receiver-initiated wireless MACs based on the perceived inter-BSS interferences.

4.2 Inter-BSS interference mitigation

Heterogeneous wireless MAC design for inter-BSS interference mitigation can be illustrated using the example shown in Figure 3. The observation is that if client 0 and 3 always initiate the channel access, there will be no hidden/exposed terminal problem since 0 and 3 always have complete and consistent channel status assessment if they are within communication range. In other words, if client 0 or 3 is the receiver, receiver-initiated MAC should be adopted. If client 0 or 3 is the sender, regular sender-initiated 802.11 MAC will do. Note that in either case the four-way handshake with RTS/CTS is unnecessary, and, therefore, can be removed to save the control overhead. In fact, under optimal channel assignment four-way handshake does help mitigate inter-BSS interferences.

Context-dependent heterogeneous MAC relies on a learning or adaptation algorithm to choose the most appropriate MAC protocol from the protocol space. Our simulation shows that very simple learning algorithms, based on the channel access success ratio, work very well in an 802.11 WLAN with inter-BSS interferences. The pseudo codes of the algorithm are shown in Figure 5. Note that whenever the MAC protocol is about to change, the node currently initiating channel access has to signal the the other node for the switching to become effective. Such signal is piggybacked in one DATA (or request) transmission in our simulation.

```
// - successRatio: recent channel access success
//          ratio
// - sf: 1 if current channel access is successful,
//          0 otherwise
// - srThreshold: min success ratio that triggers
//          switching
// - numThreshold: min number of channel access
//          attempts before switching
Switch_MAC()
1.   UpdateSuccessRatio(successRatio, sf)
2.   numberAttempts = numberAttempts + 1
3.   if ( numberAttempts > numThreshold AND
4.        successRatio < srThreshould )
5.        numberAttempts = successRatio = 0
6.        if ( currentMAC == SNDR_INITIATED )
7.             SwitchToRcvrInitiatedMAC()
8.        else if( currentMAC == RCVR_INITIATED )
9.             SwitchToSndrInitiatedMAC()
```

Figure 5: Heterogeneous MAC for inter-BSS interference mitigation

One important issue of heterogeneous MAC protocol design is the inter-operability, which is trivial with homogeneous MAC protocol. To this end, we define a single set of signaling messages (i.e., RTS/CTS/ACK/RTR) although different MAC protocols may interpret those messages differently. The new RTR (request-to-receive) message is for the receiver to poll the sender for the transmission of the next packet when receiver-initiated MAC is employed. The handshake for the receiver-initiated MAC is therefore RTR/DATA. Other nodes overhearing RTR should treat it the same as if an RTS message were received. Our receiver-initiated MAC does not send out ACK. Instead, the next RTR implicitly acknowledges the previously received packet, identified by the 802.11 MAC sequence number. The sender will then determine if a retransmission is necessary. Note that when the MAC is receiver-initiated the sender sets one

[6]Similar to 802.11 point coordination function (PCF) that is seldom supported by existing commercial 802.11 interfaces.

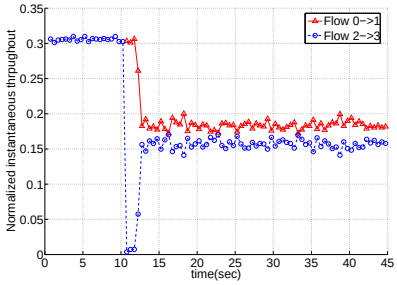


Figure 6: Normalized instantaneous throughput of flow 0→1(2-way) and 2→3(2-way)

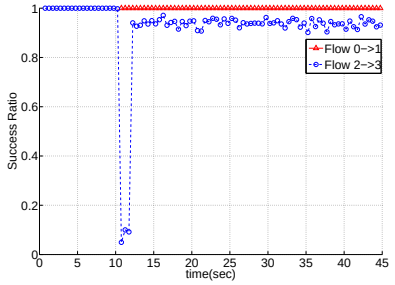


Figure 7: Normalized instantaneous success ratio of flow 0→1(2-way) and 2→3(2-way)

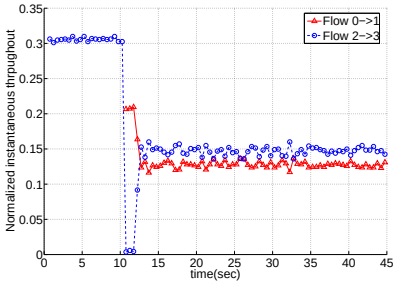


Figure 8: Normalized instantaneous throughput of flow 0→1(4-way) and 2→3(2-way)

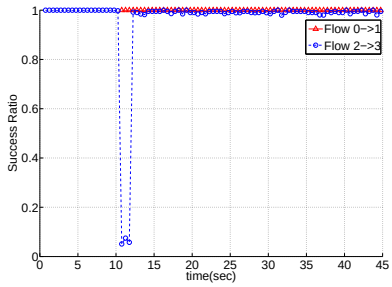


Figure 9: Normalized instantaneous success ratio of flow 0→1(4-way) and 2→3(2-way)

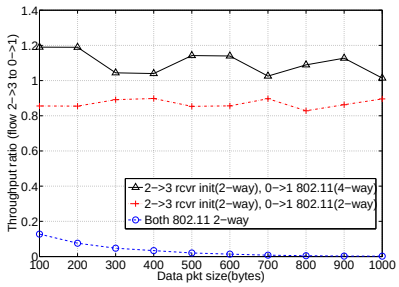


Figure 10: Throughput ratio, communication range

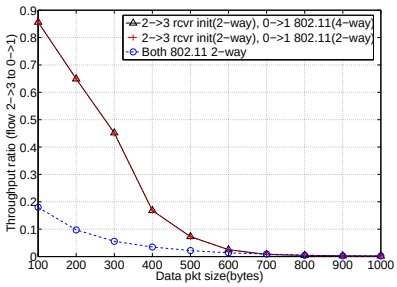


Figure 11: Throughput ratio, blocking range

bit in DATA packet header to inform the receiver if there are more packets in the queue, so that the receiver engages in proper inter-frame backoff before it polls for the next packet. The first packet arriving in an empty queue for a receiver is always transmitted using sender-initiated MAC.

Besides the stateful learning strategy as described above, we will also pursue the stateless approach. With a stateless approach, a sender and a receiver may simply alternate among all possible MAC protocols, on a per-packet basis. Collectively the channel access will be *randomized* to avoid the worst. At the cost of lower channel utilization the stateless approach is significantly simpler to design and implement. It is also more robust to malicious attacks to the learning engine that we design for the stateful approach. Given that complete information for the stateful learning might be expensive, if not impossible, to collect, a practical approach might be hybrid with the resultant MAC protocol alternates in a constrained protocol subspace, as we will explore in the future.

5. EVALUATION

We provide a preliminary evaluation of our self-learning heterogeneous MAC protocol adaptation in this section. We focus on how dynamic, heterogeneous protocol structures can help solve the unfairness resulting from exposed receiver and/or hidden sender problem. We implement receiver-initiated MAC with the current 802.11 in *ns-2* simulator version *2.28*. Throughout all the simulations Two-Ray Ground radio propagation model is used, the transmitting power is set so that the communication range is 115m, and the carrier sense threshold is set so that the default blocking range is 200m. We use 2Mbps basic rate and 11Mbps data rate based on IEEE 802.11b. Traffics are generated by continuously-backlogged CBR/UDP flows and each simulation runs for 45 seconds.

We use two metrics to evaluate the performance. **Success ratio** is the number of data packets received over the number of channel access attempts if the flow is initiated by the sender. Or, it is the number of data packets received over the number of invitation packets sent by the receiver if the flow is receiver-initiated. Success ratio can be viewed as the metric for the effectiveness of the channel access at either the sender or receiver side. **Throughput** at transport layer serves as the metric for protocol efficiency and fairness in channel access.

The well-known exposed receiver problem is shown in Figure 3(a) where sender 0 and 2 are outside the blocking range of each other. Client 3 is an exposed receiver since it is placed in the communication/blocking range of client 0, which is associated with another access point (node 1) in a neighboring BSS. Notice that in this configuration, if the transmission is initiated by the sender flow 0→1 will always succeed in the channel contention because its receiver (client 1) is not interfered by flow 2→3. We therefore study how receiver-initiated MAC can help improve fairness and keep the channel utilization high for flow 2→3.

We first run flow 2→3 from 0 to 45 seconds. At time 10, flow 0→1 is started and competes with flow 2→3. Initially both flows are sender-initiated. However, starting from time 10, flow 2→3 suffers seriously from exposed receiver problem

and success ratio dramatically decreases. The decrease in success ratio of flow 2→3 will trigger protocol change from sender-initiated MAC to receiver-initiated MAC. Figure 6 shows the normalized instantaneous throughput of 0.5 seconds over the entire simulation period, where both flows use two-way handshake. In the period of 0-10 seconds, flow 2→3 achieves the normalized throughput of 0.3. When flow 0→1 starts at time 10, the throughput of flow 2→3 drops to almost zero. After two seconds, however, flow 2→3 switches to receiver-initiated MAC, and both flows have the fair share of the medium. Figure 7 shows the instantaneous success ratio for both flows using two-way handshake. We can see that the success ratio of flow 2→3 between 10-12.5 second drops to the range of [0.05,0.1], when it suffers from the hidden receiver problem. However, it quickly restores to high success ratio when it learns to start receiver-initiated MAC. In addition, we simulate a hidden client in the BSS of flow 0→1 so that four-way handshake with RTS/CTS is adopted, while flow 2→3 continues to use two-way handshake. Figure 8 again shows the instantaneous throughput for both flows. Comparing Figure 6 and Figure 8, we observe that while flow 2→3's throughput keeps the same, the throughput of flow 0→1 decreases by 33% due to the additional RTS/CTS overhead. The corresponding normalized instantaneous success ratio is shown in Figure 9.

We then study how the data packet size will influence the effectiveness of dynamic protocol structures. Both the sender-initiated and receiver-initiated MACs use the same set of control packets (RTS,CTS,ACK,RTR) to signal the reception of data or the occurrence of transmission. Obviously, we want to keep control packets small so that the channel is used mostly for data transmission. The difference of transmission time between control and data packets will, however, have different impacts on whether the protocol is sender-initiated or receiver-initiated. We again use the topology in Figure 3(a) but directly configure flow 2→3 to be receiver-initiated and flow 0→1 sender-initiated. By fixing the control packet size and varying the data packet size, we show how this will affect the fairness of the two flows. Figure 10 shows the throughput ratio of flow 2→3 to flow 0→1 with data packet sizes ranges from 100 bytes to 1000 bytes when node 3 and node 1 are within communication range. We observe that the data packet size does not have much impact on the fairness when the two flows can communicate. Finally Figure 11 shows the results when node 3 and node 1 are out of communication range but still interfered by each other. In this case, we observe that the two flows will have fair contention when the data packet size is comparable to the control packet size, i.e. 100 bytes. We are currently working on self-learning collision avoidance to deal with this situation.

6. CONCLUSION

In this paper we analyze the interference mitigation strategies in existing 802.11 WLANs and show that incomplete and inconsistent channel status assessment due to intra-/inter-BSS interferences leads to the hidden/exposed terminal problem. We then propose a novel approach based on a class of heterogeneous MAC protocols that are not only parameter-wise adjustable, but also *structurally adaptive*. Different from existing network protocol design, our method results in dynamic, context-aware, heterogeneous MAC protocols that are usually applied on a per sender-receiver pair basis, for the same function of wireless medium access control. A set of signaling messages are defined for inter-operability among heterogeneous MACs, although they may interpret those control messages differently based on their specific context. Our experiences with heterogeneous MACs define new dimensions in the network protocol design space. The power of this method is demonstrated in that an effective and fair channel contention environment, approximate to that in a one-hop wireless LAN, can be achieved for long-term fairness in a WLAN with both intra- and inter-BSS interferences through localized mechanisms. We are currently investigating the impact of distributed learning on the global system stability, different learning algorithms and the stateless approach, and the implementation issues in a programmable radio testbed.

7. REFERENCES

[1] IEEE 802.11 task group e. http://grouper.ieee.org/groups/802/11/Reports/tge_update.htm.

[2] Place lab: A privacy-observant location system. http://www.placelab.org/.

[3] Wifi maps: Hotspot location an dwi-fi directory. http://www.wifimaps.com/.

[4] I. Aad and C. Castelluccia. Differentiation mechanisms for IEEE 802.11. In *Proceedings of IEEE INFOCOM*, 2001.

[5] A. Akella, G. Judd, P. Steenkiste, and S. Seshan. Self management in chaotic wireless deployments. In *Proceedings of ACM MobiCom*, 2005.

[6] P. Bahl, R. Chandra, and J. Dunagan. SSCH: Slotted seeded channel hopping for capacity improvement in IEEE 802.11 ad-hoc wireless networks. In *Proceedings of ACM MobiCom*, 2004.

[7] P. Bender, P. Black, M. Grob, R. Padovani, N. Sindhushayana, and A. Viterbi. CDMA/HDR: A bandwidth-efficient high-speed wireless data service for nomadic users. *IEEE Communications Magazine*, 38:70–77, Jul. 2000.

[8] V. Bharghavan. Performance evaluation of algorithms for wireless medium access. In *Proceedings of IEEE Performance and Dependability Symposium*, 1998.

[9] V. Bharghavan, A. Demers, S. Shenker, and L. Zhang. MACAW: A medium access protocol for wireless LANs. In *Proceedings of ACM SIGCOMM*, 1994.

[10] G. Bianchi. Performance analysis of the ieee 802.11 distributed coordination function. *IEEE Journal on Selected Areas in Communications*, 18(3):535–547, March 2000.

[11] C. L. Fullmer and J. Garcia-Luna-Aceves. Solutions to hidden terminal problems in wireless networks. In *Proceedings of ACM SIGCOMM*, 1997.

[12] IEEE Computer Society. Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. IEEE standard 802.11, 1999.

[13] S. Shenker. Fundamental design issues for the future Internet. *IEEE Journal on Selected Areas in Communications*, 13:1176–1188, 1995.

[14] J. So and N. H. Vaidya. Multi-channel MAC for ad hoc networks: Handling multi-channel hidden terminals using a single transceiver. In *Proceedings of ACM MobiHoc*, 2004.

[15] F. Talucci, M. Gerla, and L. Fratta. MACA-BI (MACA by invitation) a receiver oriented access protocol for wireless multihop networks. In *Proceedings of IEEE PIMRC*, 1997.

[16] X. Yang and N. H. Vaidya. On the physical carrier sense in wireless ad-hoc networks. In *Proceedings of IEEE INFOCOM*, 2005.

[17] J. Zhu, X. Guo, L. L. Yang, and W. S. Conner. Leveraging spatial reuse in 802.11 mesh networks with enhanced physical carrier sensing. In *Proceedings of IEEE ICC*, 2004.