

Asymmetric RTS/CTS in Ad Hoc Wireless LAN

Akihisa MATOBA , Masaki HANADA, Hojun MOON, Moo Wan KIM

Tokyo University of Information Sciences, Japan

mwkim@rsch.tuis.ac.jp

Abstract— A wireless network node with the Omni antenna tends to cause problems called “Hidden Node” and “Exposed Node”. RTS/CTS mechanism has been introduced to mitigate Hidden Node and most of existing researches assume that RTS and CTS are sent at the same data rate. In this paper we have intentionally allocate different transmission rate to RTS and CTS in order to mitigate effect of Exposed Node. The simulation result showed that the proposed method achieved higher throughput.

Keywords— Exposed Node, Hidden Node, IEEE802.11, Simulation, RTS/CTS

I. INTRODUCTION

A wireless network node with Omni antenna tends to cause problems called “Hidden Node” and “Exposed Node” [1]. Assuming a sender node and a receiver node, a Hidden Node

is located near to the receive node and can hear the transmission from the receiver while it cannot hear the transmission from the sender as it is far enough from the sender. The Hidden Node and the sender can send a frame respectively at the same moment and can cause a collision at the receive node. An Exposed Node is located near the sender and its transmission reaches to the receiver as it is far enough from the receiver. The Exposed Node doesn't cause a collision at the receiver when it sends a frame at the same moment when the sender sends a frame. But due to carrier sense mechanism of IEEE802.11, the Exposed Node detects a transmission of the sender and has to suspend the transmission. This may cause unnecessary transmission suspensions and degrade network performance. Even it can cause pseudo dead-lock situation in network [2].

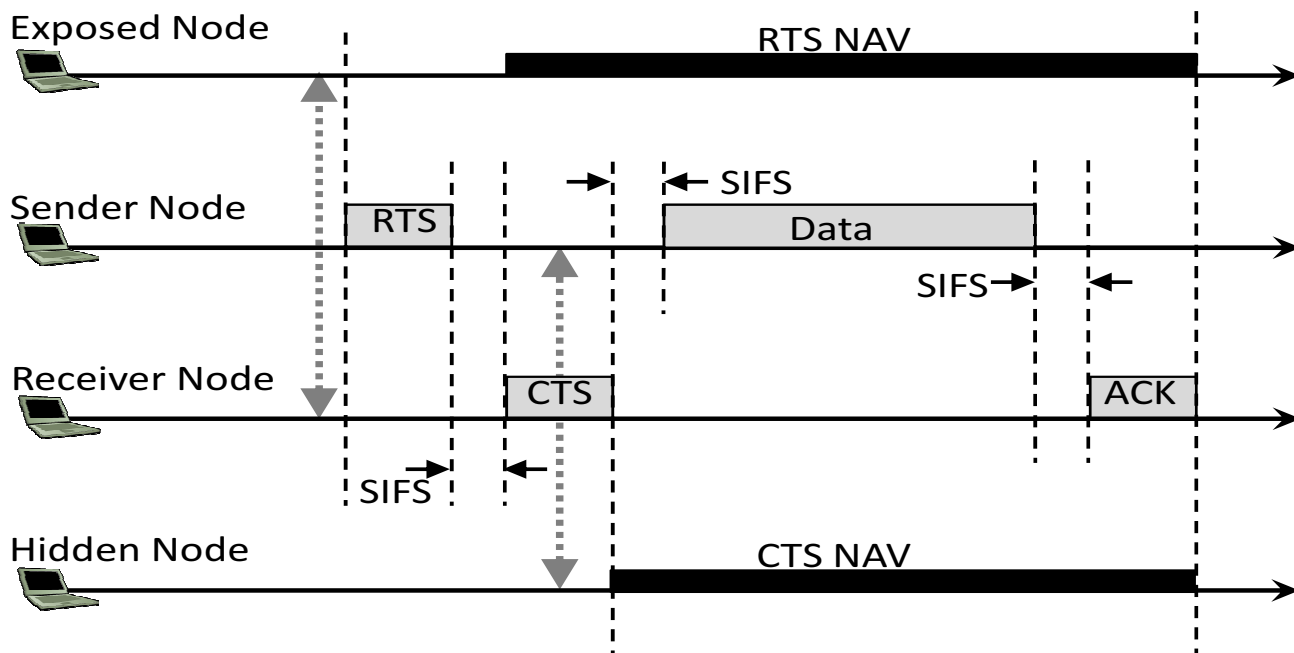


Figure 1. RTS/CTS Mechanism

RTS/CTS mechanism as shown in Figure 1 has been introduced to mitigate Hidden Node since the first version of IEEE802.11. A sender sends RTS (Request To Send) frame first and NAV in the RTS reserves air time of any nodes which hear the RTS. Those nodes must suspend their transmission until the receiver sends ACK to the sender. The receiver node sends back CTS (Clear To Send) frame after it receives RTS. CTS also have NAV and suspend transmission of nodes which hear the CTS until the receiver sends ACK. Then the sender sends a data frame after it receives CTS and the receiver sends ACK after it receives the data frame. In this mechanism, Hidden Nodes around the receiver can suspend transmissions by the CTS and the receiver can avoid collisions to receive the data frame. But this mechanism creates Exposed Nodes around the sender as they hear the RTS and suspend their transmission. This is necessary to protect the CTS and the ACK to be received at the sender safely, but entire NAV period is too long to suspend.

II. BASIC IDEA AND RELATED WORKS

Various researches have been conducted to mitigate Exposed Node and Hidden Node [3].

The most of existing researches assume that RTS, CTS and Data are sent at the same data rate and have the same radio coverage. This was true with the first version of IEEE802.11, but now Data frame is sent at multi rates (54Mbps with 11a/g at maximum) while control frames such as RTS/CTS remain

the lowest basic rate (1Mbps with 11g, 6Mbps with 11a). There are some researches to consider multi rate but no researches assume asymmetric transmission rate to RTS and CTS. Our research we intentionally allocate different transmission rate to RTS and CTS in order to proactively control the radio coverage and mitigate effect of Exposed Node. We redefined the objective of RTS only to provoke CTS. RTS needs to reach to receiver but it doesn't need to reach to any other nodes. So the RTS should be sent at the maximum data rate as data frame. This strategy introduces risk to lose CTS and ACK at the sender by collisions from surrounding nodes (Exposed Nodes). But we assume this risk is minimal as CTS and ACK have short length in comparison to data frame, and highly loaded environments which cause collisions to CTS or ACK also causes collision at RTS and data transmission may not be achievable anyway.

As shown in Figure 2, higher transmission rate of RTS makes the RTS coverage smaller than CTS and reduces Exposed Node. In order to avoid collision of data frame at the receiver, CTS should be sent at lowest data rate to be heard by Hidden Node as many as possible. In case if RTS range is completely included in CTS range, there is no Exposed Node.

By the way above discussion to reduce radio coverage is not applicable to NAV and is not applicable to CCA. Any frames have PLCP preamble and header with 1Mbps, and the payload portion is in higher data rate (e.g. 54Mbps) and NAV is in the payload. The effect of CCA may need to be investigated further.

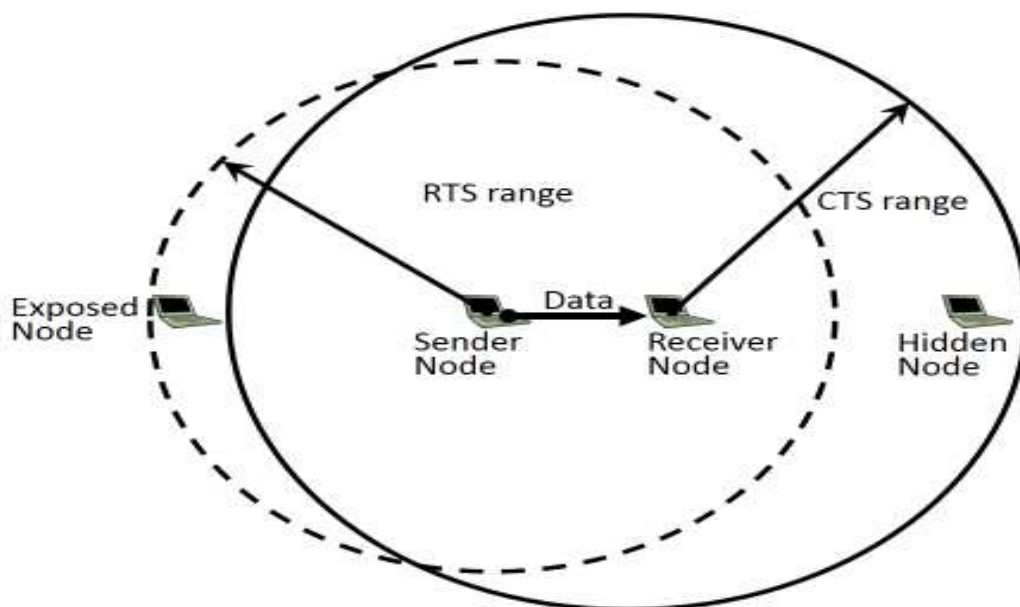


Figure 2. Concept of Asymmetric RTS/CTS

TABLE 1. SIMULATION PARAMETERS

Frame	Type	Data Rate	Range
	RTS	18Mbps	88m, 1 hop
	CTS	6Mbps	140m, 2 hops
	Data	18Mbps	88m, 1 hop
	ACK	18Mbps	88m, 1 hop
Load	3Mbps per node with exponential distribution		
Data Size	1,000 bytes		
Distance	Nodes are located at 70m interval in a grid.		
Other	Other parameters follow 802.11a standard.		

III. EVALUATION BY SIMULATION

We conducted simulation to evaluate our proposed method. 802.11a is assumed with the parameters in the Table 1. In the simulation we configured grid of nodes and each node is placed 70m apart as in the Figure 3. In this configuration there are no Exposed Nodes. The sizes of the simulated grids are 9 nodes (3 x 3) to 225 nodes (25 x 25).

Traffic is generated at each node and sent to one of four adjacent nodes randomly. For example in Figure 3, the node 13 sends to one of node 8, 12, 14, or 18 at random. Grey nodes in the Figure 3 are Exposed Nodes if we would use standard RTS/CTS. We simulated both standard and our asymmetric RTS/CTS for comparison.

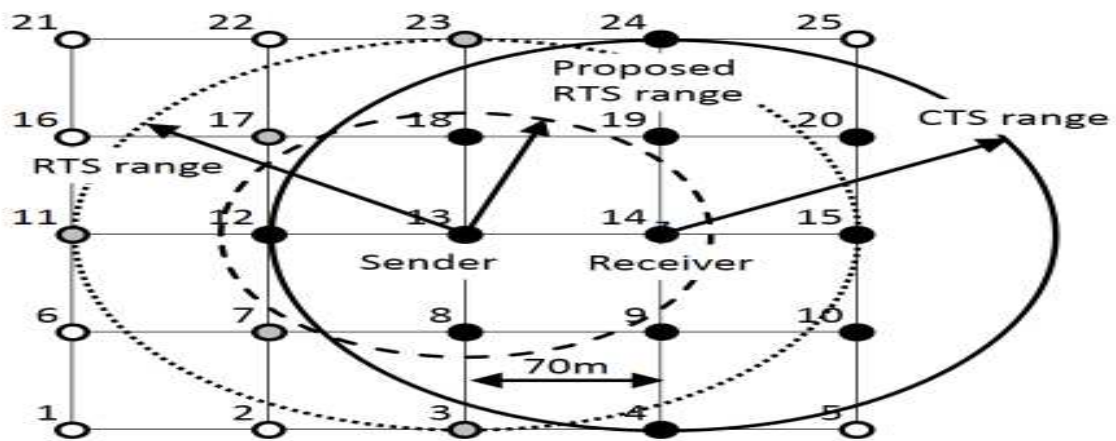


Figure 3. 25 Nodes (5 x 5) Example

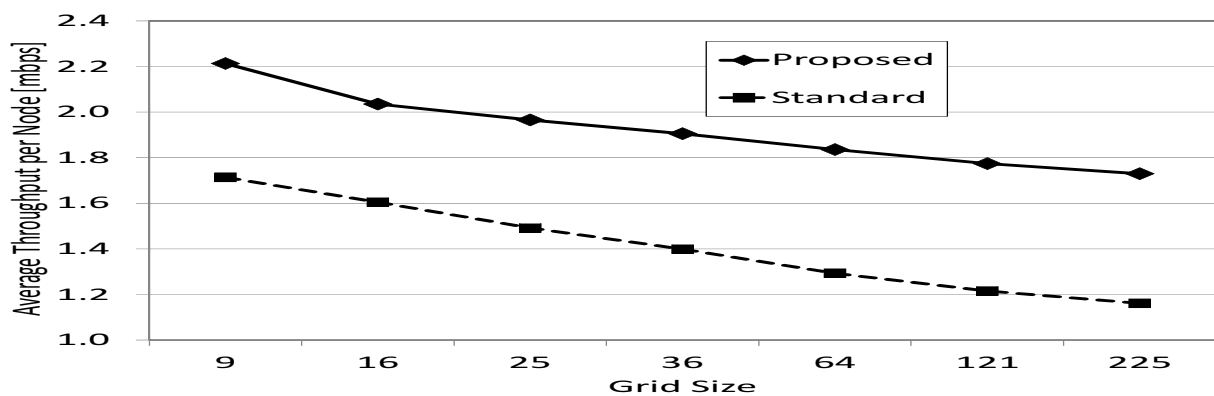


Figure 4. Average Throughput per Node by Grid Size

The simulation result showed that the proposed method achieved 30% to 50% higher throughput per node in all grid sizes as in the Figure 4. In a simulated grid, throughputs of all nodes have large dispersion, especially in small size grid.

The proposed method has an effect to reduce this dispersion as in the Figure 5. This is very preferable nature as lower throughput nodes get bigger improvement effect.

Also we found that collision of standard method is 11 to 13% and increases as grid size increases as in the Figure 6. The vertical axis shows number of transmission to send one data frame. The proposed method has stable collision of 5 to 6% and this doesn't change when grid size increases. RTS/CTS are known to reduce collisions under highly loaded network and the proposed method is also effective in this aspect.

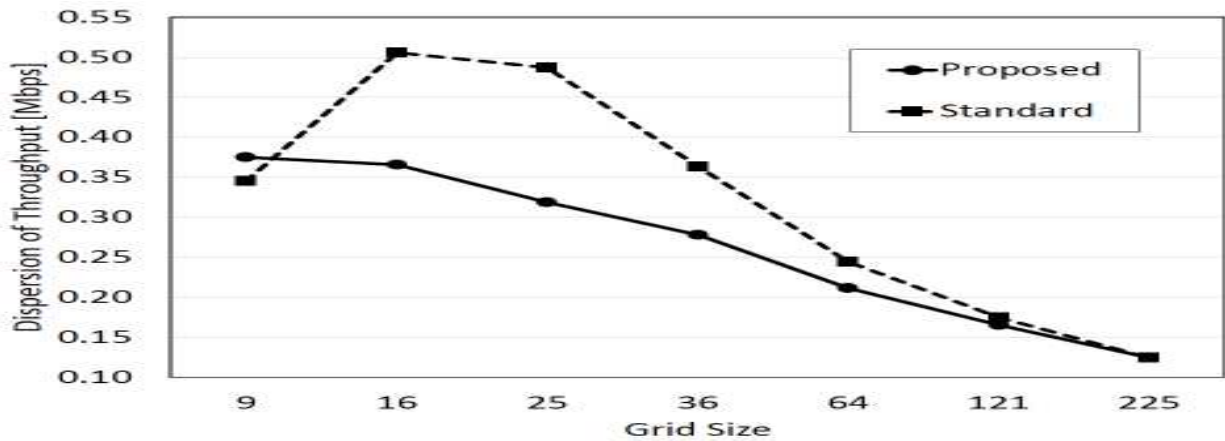


Figure 5. Dispersion of Throughput by Grid Size

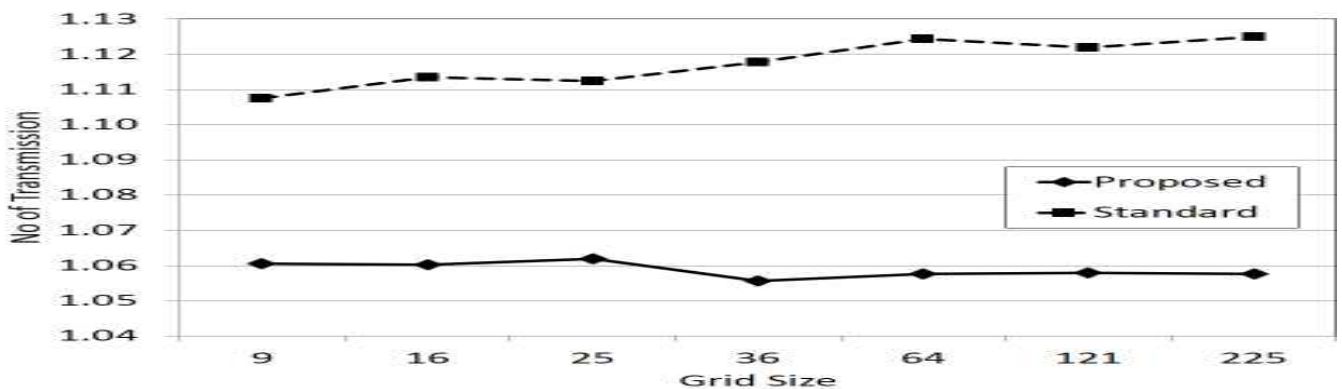


Figure 6. Collisions by Grid Size

IV. CONCLUSIONS

In our research we showed that the proposed method can improve throughput per node by 30 to 50%. We need to investigate further to validate effect of asymmetric data rate strategy and find method of selecting appropriate parameters as well as theoretical explanation.

REFERENCES

- [1] K. Xu, M. Gerla, and S. Bae, "How effective is the IEEE802.11 RTS/CTS Handshake in Ad Hoc Network?" Proc. IEEE Globe Com'02, pp.72-76, Nov. 2002.
- [2] S. Ray, J. B. Carruthers, and D. Starobinski, "RTS/CTS-Induced Congestion in Ad Hoc Wireless LANs," WCNC 2003 IEEE, vol. 3, pp.1516-1521, March 2003
- [3] K. Nishide, H. Kubo, and R. Shinkuma, Detecting Hidden and Exposed Terminal Problems in Densely Deployed Wireless Networks, IEEE Transactions on Wireless Communications, vol. 11, no. 11, pp.3841-3849, November 2011