Global Congestion Attacks on Wi-Fi Networks via Interference Coupling

BOSTON UNIVERSITY

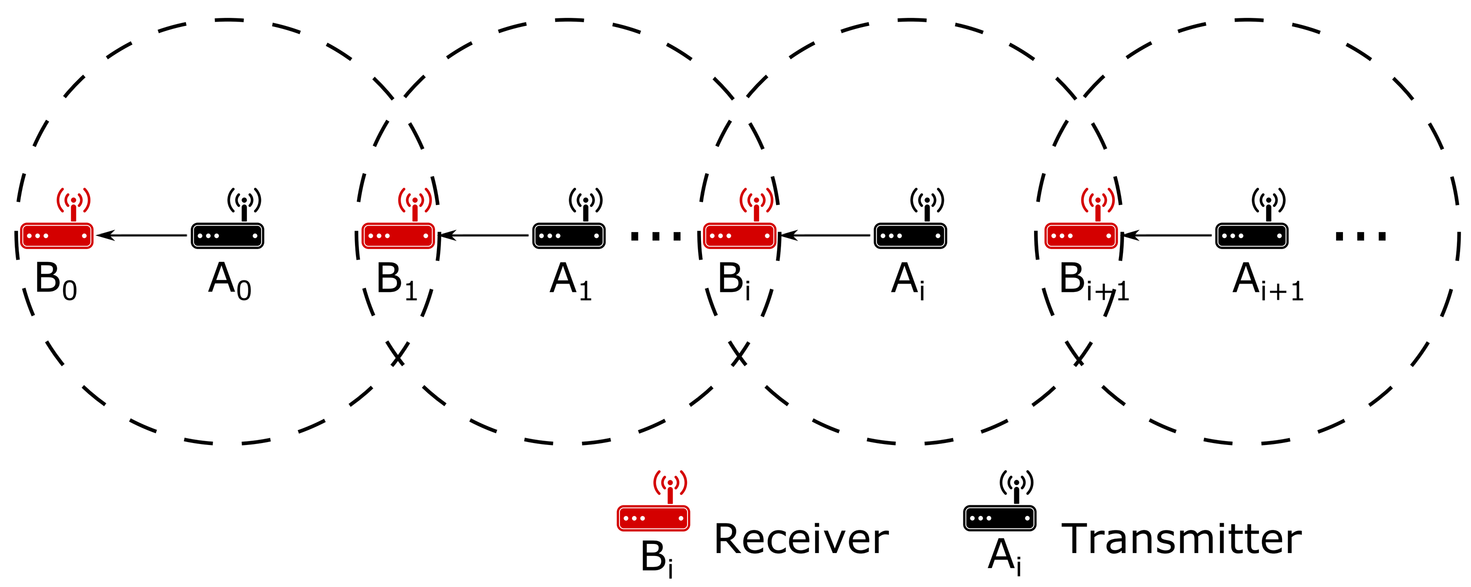
Liangxiao Xin[1], David Starobinski[1], and Guevara Noubir[2]
[1]Division of Systems Engineering, Boston University
[2]College of Computer and Information Science, Northeastern University

Northeastern University

Abstract

Hidden nodes can lead to serious channel congestion in Wi-Fi (IEEE 802.11) networks. Such vulnerability of Wi-Fi networks can be utilized by attackers to achieve a global denial of service attack, through an interference coupling phenomenon whereby collisions induced by a hidden node lead other hidden nodes to retransmit and congest the channel. In this paper, we demonstrate the feasibility of a remote and protocol-compliant interference coupling attack in Wi-Fi networks. Our results, supported by testbed experiments and NS-3 simulations, provide a feasible scenario for a local attack to propagate in space and time and cause a congestion collapse of the entire network. The results show that the retry limit and the load of node play important roles in the success (and prevention) of interference coupling attacks.

Network



- Node A_i transmits packets to B_i.
- Node A_i is a hidden node with respect to A_{i+1}. A collision happens at node B_i when A_i and A_{i+1} transmit simultaneously.
- RTS/CTS is disabled.

Attack

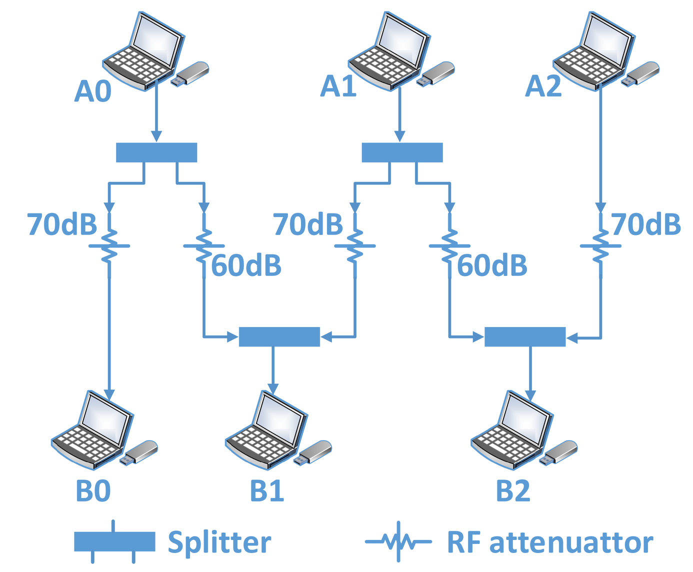
✓ Node A_0 can trigger a phase transition, resulting in a congestion collapse over the entire network.

We start by increasing the rate at which node A_0 transmits packets over its channel, in compliance with the IEEE 802.11 standard.

The transmissions by node A_0 cause packet collisions at node B_1. These collisions require node A_1 to retransmit packets. The increased rate of packet transmissions by node A_1 impact node A_2 and so forth.

This effect keeps propagating and amplifying, resulting a network-wide denial of service.

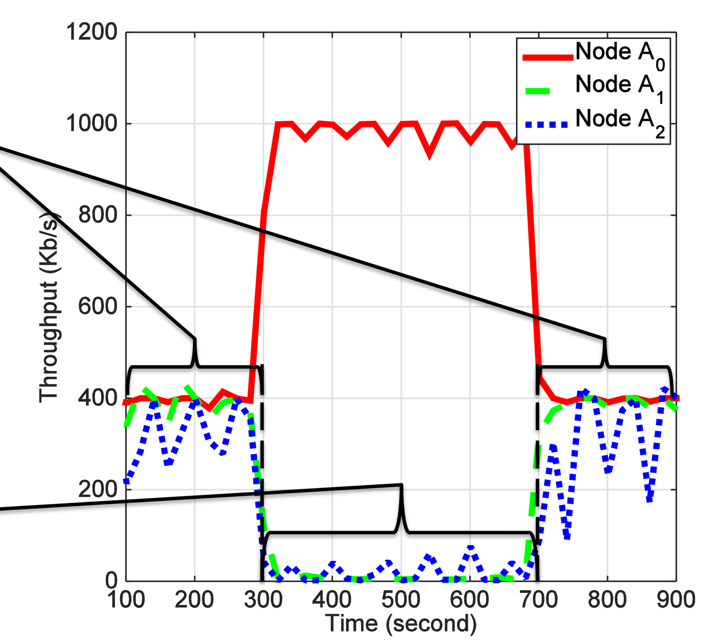
Experimentation Testbed and Result



# Tx pairs	3
Wi-Fi Card	TP-LINK TL-MN722N
Protocol	IEEE 802.11n ad hoc
Packet	1500 bytes UDP
Tx Power	0 dBm

When node A_0, A_1, and A_2 transmit at 400 Kb/s, the throughput of all the nodes remain in the vicinity of 400 Kb/s.

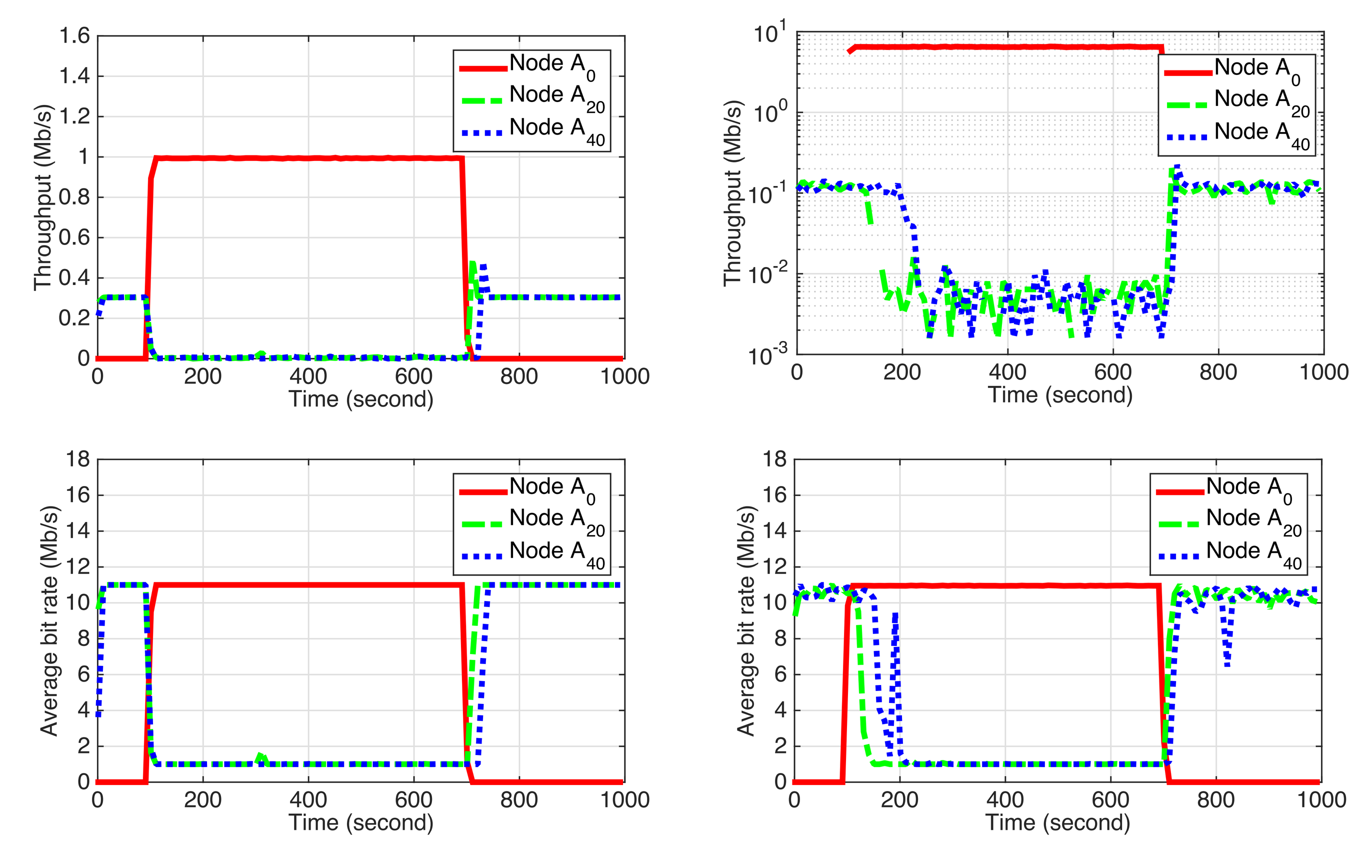
When node A_0 increases its transmission rate to 1 Mb/s, the throughput of nodes A_1 and A_2 vanish.



NS-3 Simulations under Minstrel RAA

# Tx pairs	40
Packet	2000 bytes UDP
Propagation Loss between A_i and B_i, A_i and B_{i+1}	80 dB, 70 dB
Transmission Power	40 mW
In AP mode, nodes A_i are stations and nodes B_i are access points.	

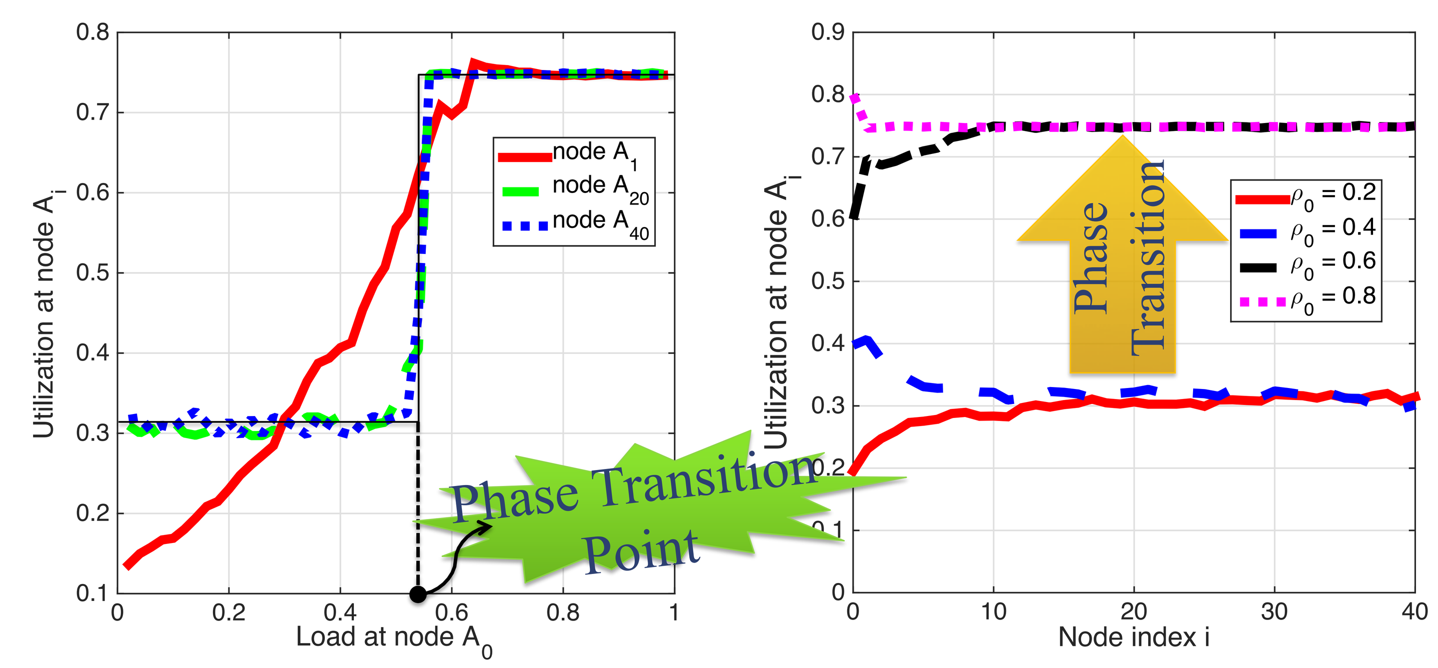
Ad hoc mode | AP mode



When node A_0 transmits, the throughput of nodes A_{20} and A_{40} vanish. Their average bit rates reduce to 1 Mb/s.

NS-3 Simulations at Lowest Bit Rate (1Mb/s)

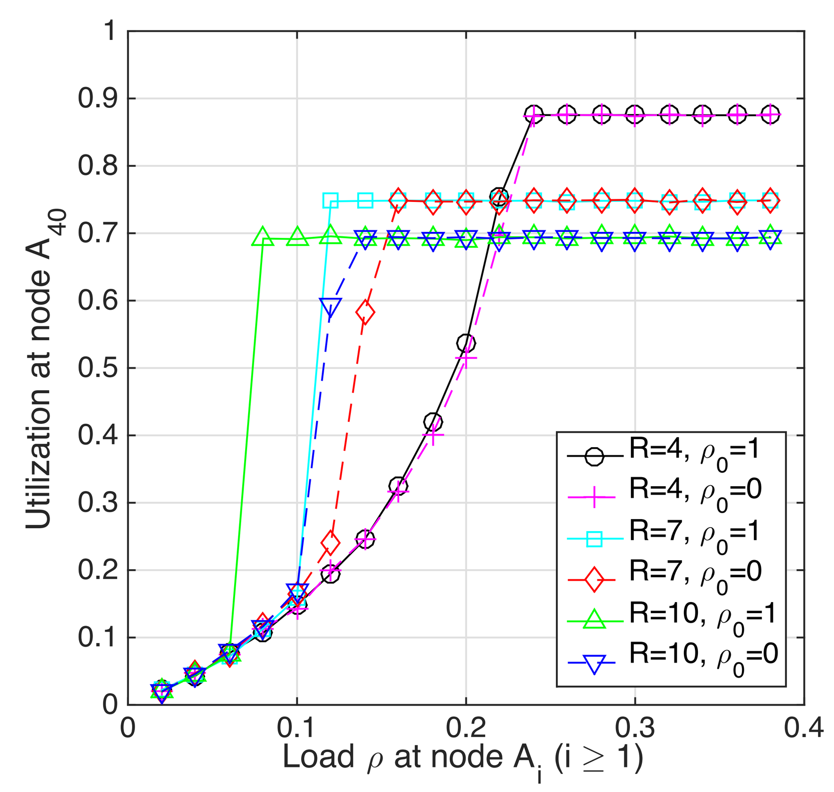
Retry Limit R = 7



As the (exogenous) load at node A_0 increases, the utilization of remote nodes (e.g., A_{20} and A_{40}) exhibits a phase transition.

The utilization converges as i gets large. When the load at node A_0 changes from 0.4 to 0.6, the sequence of utilization converge to different limits.

Different Retry Limit



Retry limit (R)	Region of load ρ in which a phase transition occurs.
R = 4	No phase transition
R = 7	$\rho \in (0.12, 0.16)$
R = 10	$\rho \in (0.08, 0.14)$

- A phase transition only occurs when the retry limit is large.
- A region of (exogenous) load exists in which a phase transition occurs.
- The size of the phase transition region increases with retry limit.

Conclusion

✧ Interference coupling attacks are feasible in Wi-Fi networks.

✧ A small change in the traffic rate of the attacker can lead to a phase transition of the entire network, from uncongested state to congested state.

✧ The phase transition only occurs when the retry limit is larger than 7.

Acknowledgment

This work was supported in part by the National Science Foundation under grant CNS-1409053.