Global Congestion Attacks on Wi-Fi Networks via Interference Coupling

Liangxiao Xin\textsuperscript{1}, David Starobinski\textsuperscript{1}, and Guevara Noubir\textsuperscript{2}
\textsuperscript{1}Division of Systems Engineering, Boston University
\textsuperscript{2}College of Computer and Information Science, 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.

Attack

- 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.

We start by increasing the rate at which node $A_{i}$ transmits packets over its channel, in compliance with the IEEE 802.11 standard.

The transmissions by node $A_{i}$ cause packet collisions at node $B_{i}$. These collisions require node $A_{i}$ to retransmit packets. The increased rate of packet transmissions by node $A_{i}$ impact node $A_{j}$ and so forth.

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

Experimentation Testbed and Result

When node $A_{0}$, $A_{1}$, and $A_{2}$ transmit at 400 Kbps/s, the throughput of all the nodes remain in the vicinity of 400 Kbps/s.

When node $A_{i}$ increases its transmission rate to 1 Mbps, the throughput of nodes $A_{i}$ and $A_{j}$ vanish.

NS-3 Simulations under Minstrel RAA

<table>
<thead>
<tr>
<th># Tx pairs</th>
<th>40</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet</td>
<td>2000 bytes UDP</td>
</tr>
<tr>
<td>Propagation Loss between $A_{i}$ and $B_{i}$</td>
<td>80 dB, 70 dB</td>
</tr>
<tr>
<td>Transmission Power</td>
<td>40 mW</td>
</tr>
<tr>
<td>In AP mode, nodes $A_{i}$ are stations and nodes $B_{j}$ are access points.</td>
<td></td>
</tr>
</tbody>
</table>

When node $A_{0}$ transmits, the throughput of nodes $A_{20}$ and $A_{40}$ vanish. Their average bit rates reduce to 1 Mb/s.

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.