

Distinguishing DoS Flooding from Hidden Terminal Collisions

Devanjali Das
Mohammad Rehman
Yacine Saoudi

COMP4203

Problem Overview

Hidden Terminal Problem

- Two nodes that can't sense each other both transmit to the AP at the same time
- Packets collide, triggering backoff and dropping throughput

DoS Flooding Attack

- Attackers floods the AP with auth requests
- AP reserves memory for each one, and legitimate users get blocked

- Both conditions cause increased packet arrivals, collisions, and reduced throughput
- The AP needs to tell them apart, and respond to each differently

Background: DoS Attack

The Attack

- Attacker floods the AP with auth requests using spoofed MAC addresses
- Each request consumes space in the AP's buffer
- Attacker never completes the handshake, so entries never clear
- Buffer fills up and legitimate users get blocked

The Solution

Elhigazi et al. — Authentication Flooding DOS Attack Detection and Prevention in 802.11 (IEEE SCORed, 2020)

- This paper proposes that a MAC filter buffer tracks requests per MAC address
- First request from a MAC gets a response and is logged
- Repeat requests will increment a counter instead
- Monitoring thread runs every 3 seconds
 - Any MAC over 5 requests gets blacklisted
- The paper finds a 98.5% improved detection rate

Background: Hidden Terminal Problem

The Problem

- Two stations can't sense each other, but both communicate with the same AP
- Simultaneous transmissions collide at the AP, causing packet loss
- Collisions trigger exponential backoff, reducing throughput
- This is caused by the network topology itself

The Solution

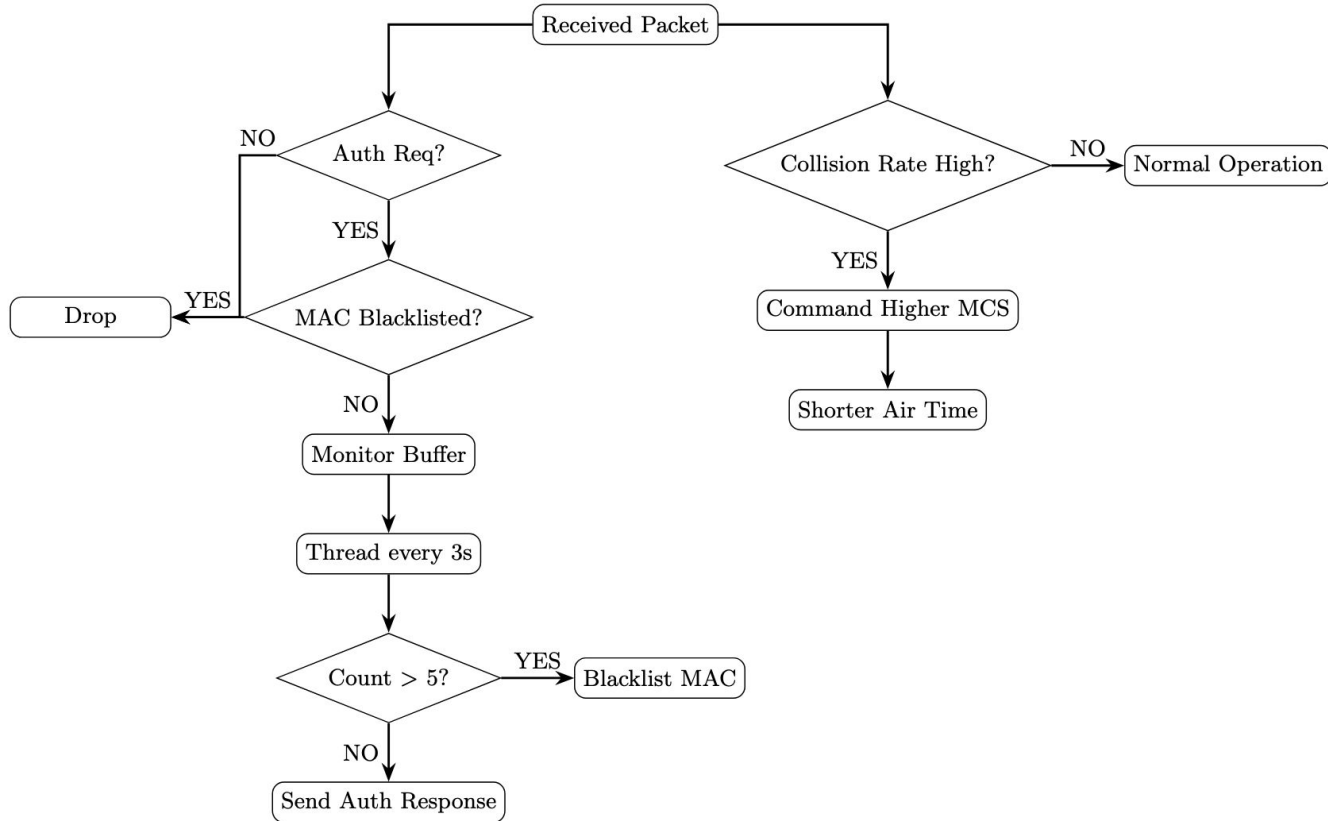
Tamai et al. — Recognition and Countermeasure to Hidden Terminal Problem by Packet Analysis in Wireless LAN (IEEE, 2020)

- The paper proposes the AP monitors collision rate directly instead of relying on stations to self-manage
- When a hidden terminal situation is detected, the AP tells stations to use a higher MCS
- This means a faster transmission, and shorter air time, lessening the chance of an overlap

Research Question

- When both problems happen at the same time, can the AP tell them apart?
- DoS Detection
 - The AP tracks how many requests come from each MAC
 - If any MAC sends more than 5 in 3 seconds, it gets blacklisted
- Collision Response
 - The AP watches for collisions and tells all stations to transmit faster to reduce the chance of two packets overlapping
- The Interaction
 - Does transmitting faster make the flooding harder or easier to detect?
- We propose an Adaptive AP that runs both systems simultaneously to distinguish between and handle each problem

Adaptive AP



Simulation Design

- Python simulation with a few nodes, an attacker, and an Adaptive AP managing both problems at once

Nodes and Network

- Nodes with positions and transmission ranges
- One node acts as an attacker
- Nodes check if the channel is free before sending

Access Point

- Tracks requests per MAC
- Blacklists anything suspicious
- Adjusts transmission speed when collisions spike

Hidden Terminal

- Two nodes that can't hear each other
- Both sending to the same AP

Visualization

- Live network view using matplotlib and networkx
- Highlights collisions and blocked nodes as they happen
- Alternatively, a TUI displaying real time stats and events in the terminal

Evaluation

- We compare three AP setups:
 - Standard
 - MAC filtering only
 - Adaptive

Metric	Standard AP	MAC Filtering Only	Adaptive AP
<i>Auth Pass Rate</i>	Drops to near 0%	Expected to be maintained	Expected to be maintained
<i>Collision Rate</i>	Stays high	Expected to stay high	Expected to decrease
<i>Detection Latency</i>	No detection	Expected < 3 seconds	Expected < 3 seconds
<i>Throughput</i>	Severely degraded	Expected partial improvement	Expected closest to baseline

The goal would then be to differentiate malicious attacks from unintentional collisions while maintaining throughput

Thank You For Listening!