ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

TELE KOM AUS TRIA

LANCASTER UNIVERSITY

Lightweight Detection of Malicious Traffic in Wireless Mesh Networks

Fabian Hugelshofer

Supervisors: P. Smith, N. Race, D. Hutchison

Multi Service Networks 2008

Overview

- Problem statement
- Preliminary performance analysis
- OpenLIDS
- Conclusions

Motivation

- Malware in Wireless Networks [STONE08]
  - Analyse wireless network of 67th IETF meeting 2006
  - Worm propagation & DOS attacks cause high channel utilisation
    - Retransmissions (50% of traffic)
    - Reduced throughput and high RTT
    - Jamming of management frames
- Shared wireless medium
  - Collisions & contention
  - Auto rate fallback
  - Multiple channel usage for multi hop
- Shared internet connections
  - Typically asymmetric with smaller upload
- **Detect malicious traffic to avoid congestion**

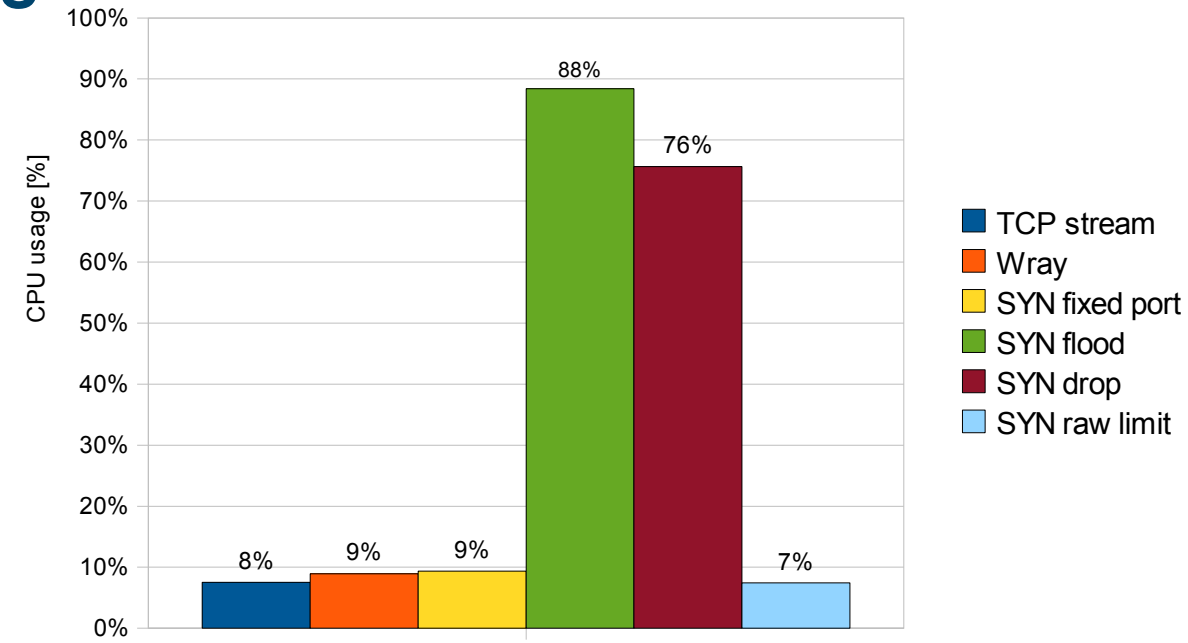
WMN Problems

- Decentralised internet uplinks
- No dedicated hardware
- Client-based approaches not feasible
- **Ability to use existing mesh boxes for detection?**
  - Restricted hardware resources
  - Negear WG302: 266Mhz, 32MB RAM, 8MB Flash, IEEE 802.11g
  - OpenWRT (Linux for network devices)
- Automated remediation
  - High certainty required
  - Robustness against misuse (DoS)

Preliminary Performance Analysis

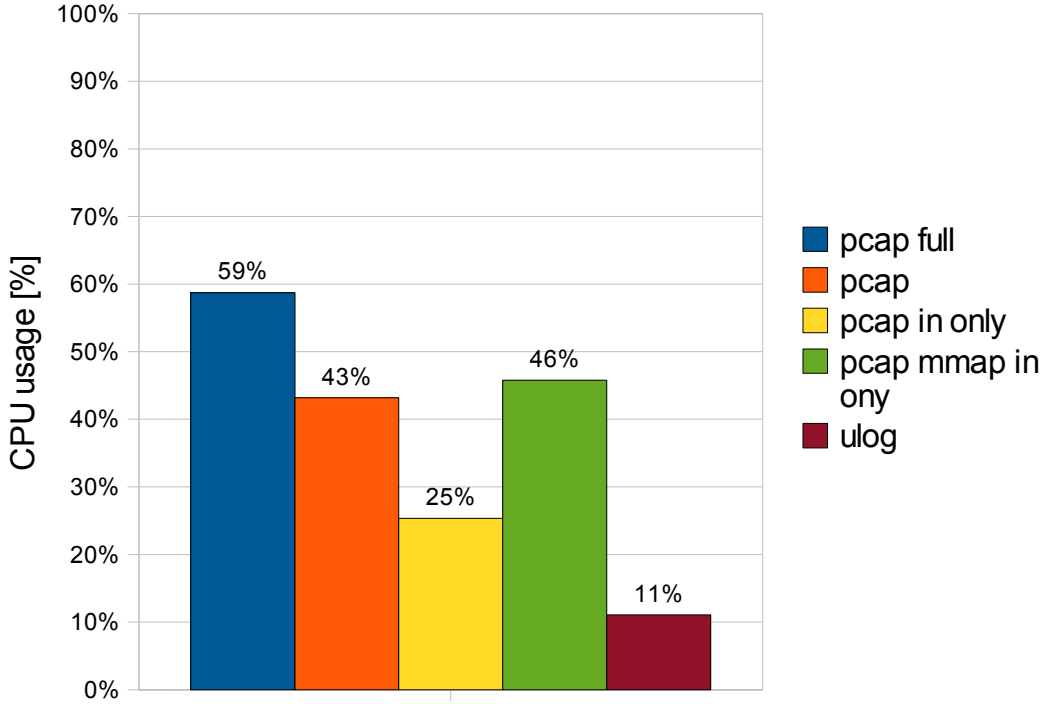
- Wireless 2-hop setting
- Performed at maximum throughput (max. 13 Mbps)
- Traffic sources
  - Single TCP stream with big packets (Netperf)
  - Replay traffic from Wray Community WMN
  - SYN flood

Routing



- High CPU usage on high number of new flows
  - Netfilter connection tracking gets stressed
- Dropping in filter table does not help
  - Conntrack still allocated but not stored
- Drop in raw table before connection tracking

Packet Capturing



- Traffic source: Netperf TCP stream
- Packet drops with standard libpcap
- Bro & Snort: 100% CPU usage, 75% packet drops

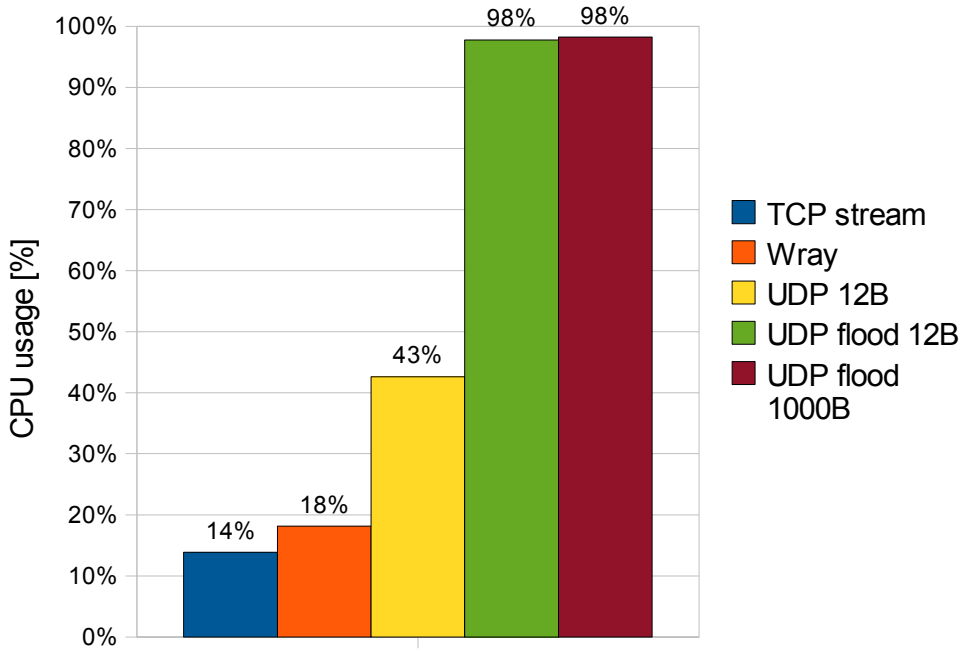
Lightweight Intrusion Detection System (OpenLIDS)

- Anomaly based
- Simple counters per host
- Detailed analysis if thresholds are reached
  - Verify alert
  - Identify malicious flows as fine grained as possible
- Connection tracking events from kernel
  - Avoid having to do expensive work twice
  - Flow statistics & timeouts

Detection Metrics

- Scanning (e.g. Worm Propagation) [WAGNER06]
  - Failed connection attempts (TCP RST, ICMP unreachable, timeout)
  - Check if many failed attempts to distinct hosts on the same port
- Denial of Service Floods [WAGNER06]
  - Failed connection attempts
  - Check if many failed attempts to same host
- SPAM Bots (UCE, MMW) [MUSASHI04]
  - High number of SMTP flows
  - High SMTP data volume
  - DNS MX queries if own SMTP engine is used
- IP spoofing
  - Only for directly connected hosts (MAC visible)

OpenLIDS Basic Counting Performance



- Small packets cause bigger load
- Packet drops during UDP flood (10% 1000B, 88% 12B)
  - Connection tracking & event communication overhead
  - Limit host with high number of flows on high CPU usage

Conclusions

- Malicious traffic should be blocked
- Resources on mesh box limited
- Cheap detection metrics possible
  - Detect: Scanning, Flooding, Spamming
  - Problems: Connection tracking & packet capturing
  - Solutions: Use kernel connection tracking & Netfilter ULOG
- Attacks on higher layers difficult to detect
  - Other cheap metrics too uncertain for automated response
    - Destination Entropy, Number of flows, Flow size, In/Out-Ratio, ...
  - Expensive metrics likely too expensive
    - Pattern matching, Content statistics, ...

Thank you!

- [STONE08] B. Stone-Gross, C. Wilson, K. Almeroth, E. Belding, H. Zheng, and K. Papagiannaki. Malware in IEEE 802.11 Wireless Networks. In Proceedings of the Passive and Active Measurement Conference (PAM), 2008.
- [WAGNER06] A. Wagner, T. Dübendorfer, R. Hiestand, C. Göldi, and B. Plattner. A Fast Worm Scan Detection Tool for VPN Congestion Avoidance. Lecture notes in computer science. 2006.
- [MUSASHI04] Y. Musashi, R. Matsuba, and K. Sugitani. Indirect Detection of Mass Mailing Worm-Infected PC terminals for Learners. Proc. ICETA2004, 2004.