Fusing Beliefs of Multi-Layer Metrics for Detecting Security Attacks

Konstantinos Kyriakopoulos
Francisco J. Aparicio Navarro
David Parish

Loughborough University

Cosener's House - July 2011

Overview

- Introduction
- Aims
- Metrics - Methodology
- Data Fusion: D-S
- Examined Attacks
- Detection Results
- Conclusions - Future Work

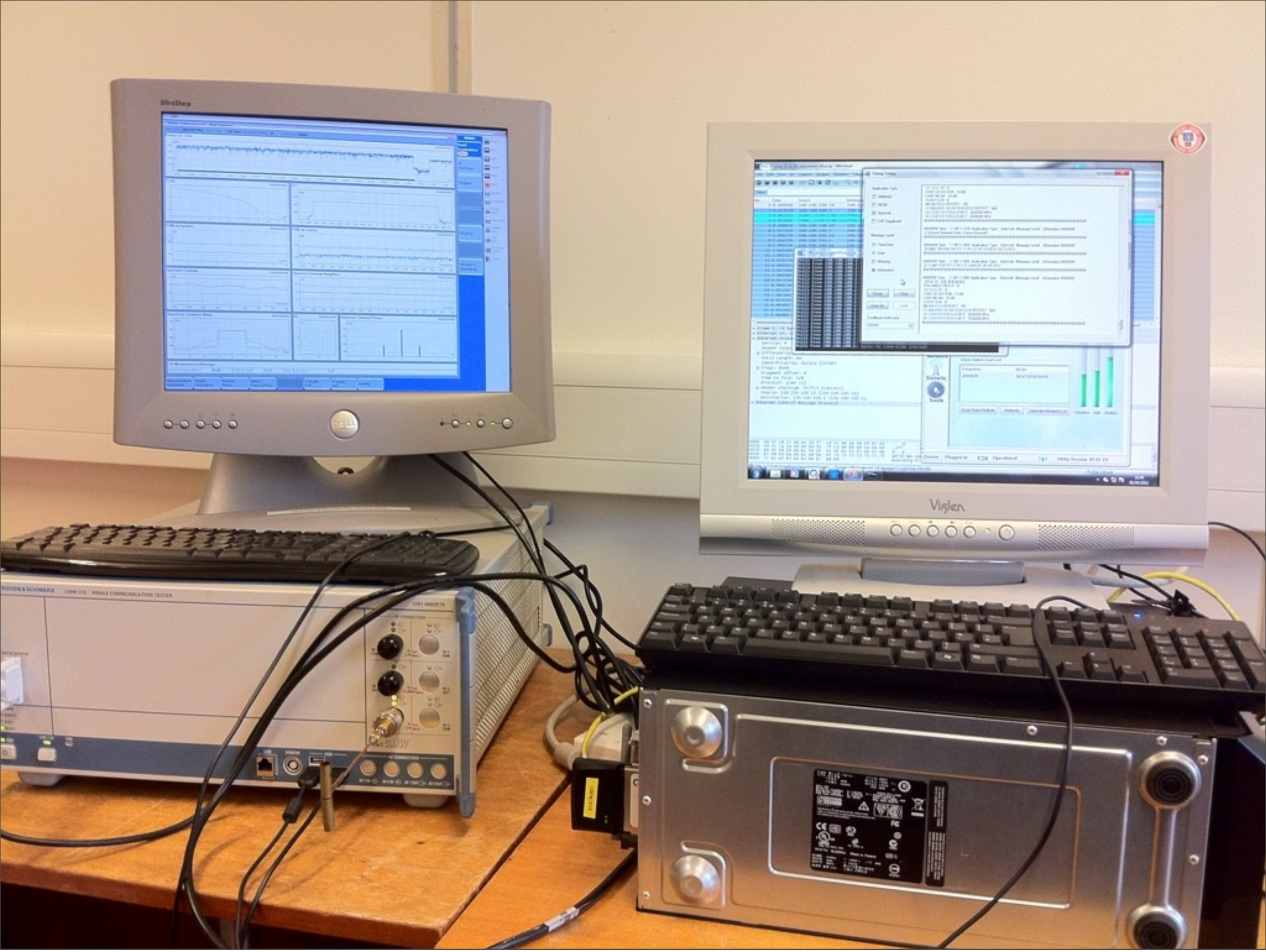
Introduction

- Wireless Network increasingly at risk.
- Current IDS tools focus on one layer or do not utilise metrics intelligently.
- Performance of single metric can be poor.
- Multi-layer approach may result in higher detection accuracy.

Aims

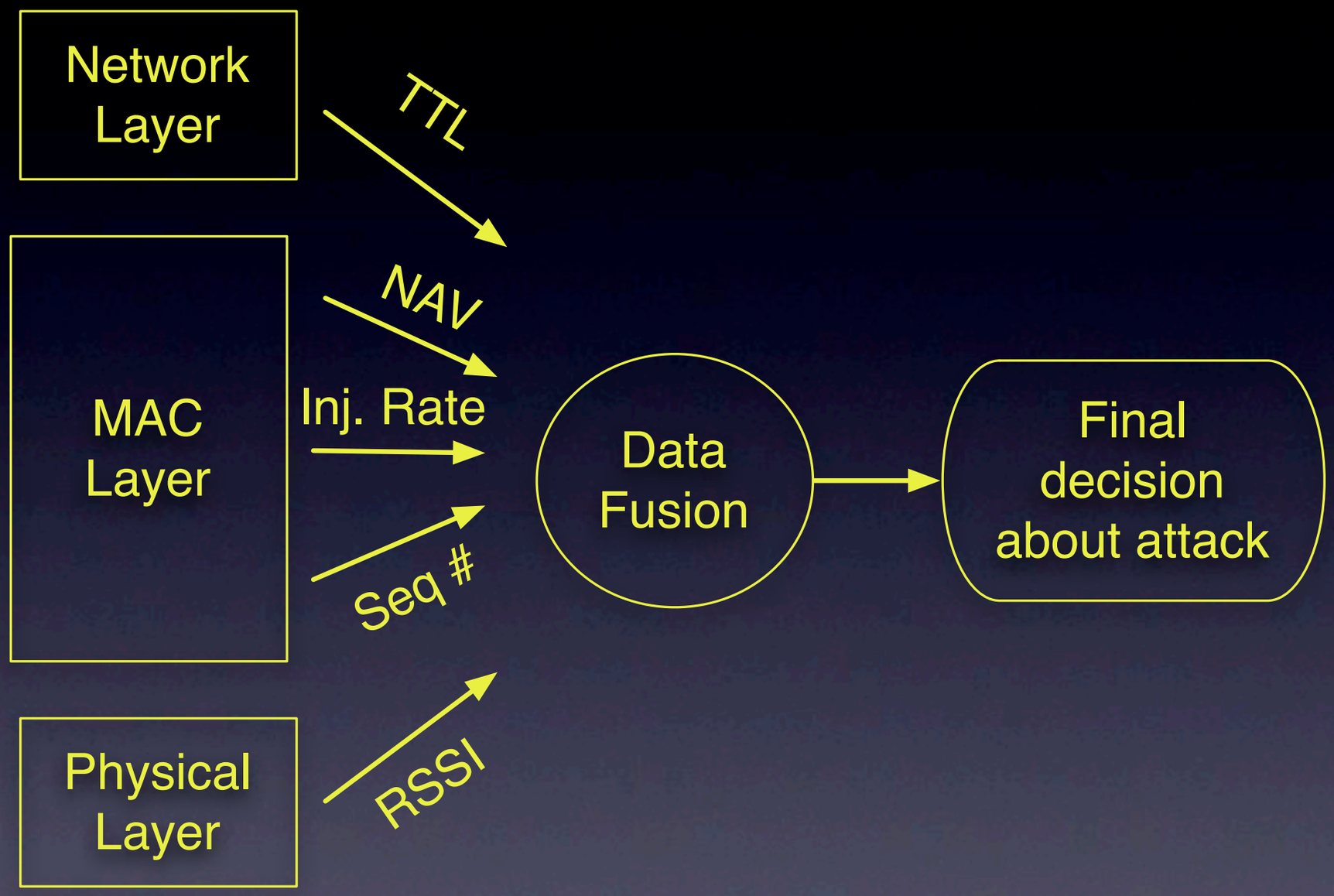
- Collect metrics from multiple layers
- Combine metrics using Data Fusion
- Better accuracy from conventional methods

- Concept:
  - low cost
  - scalable
  - applicable to other wireless technologies



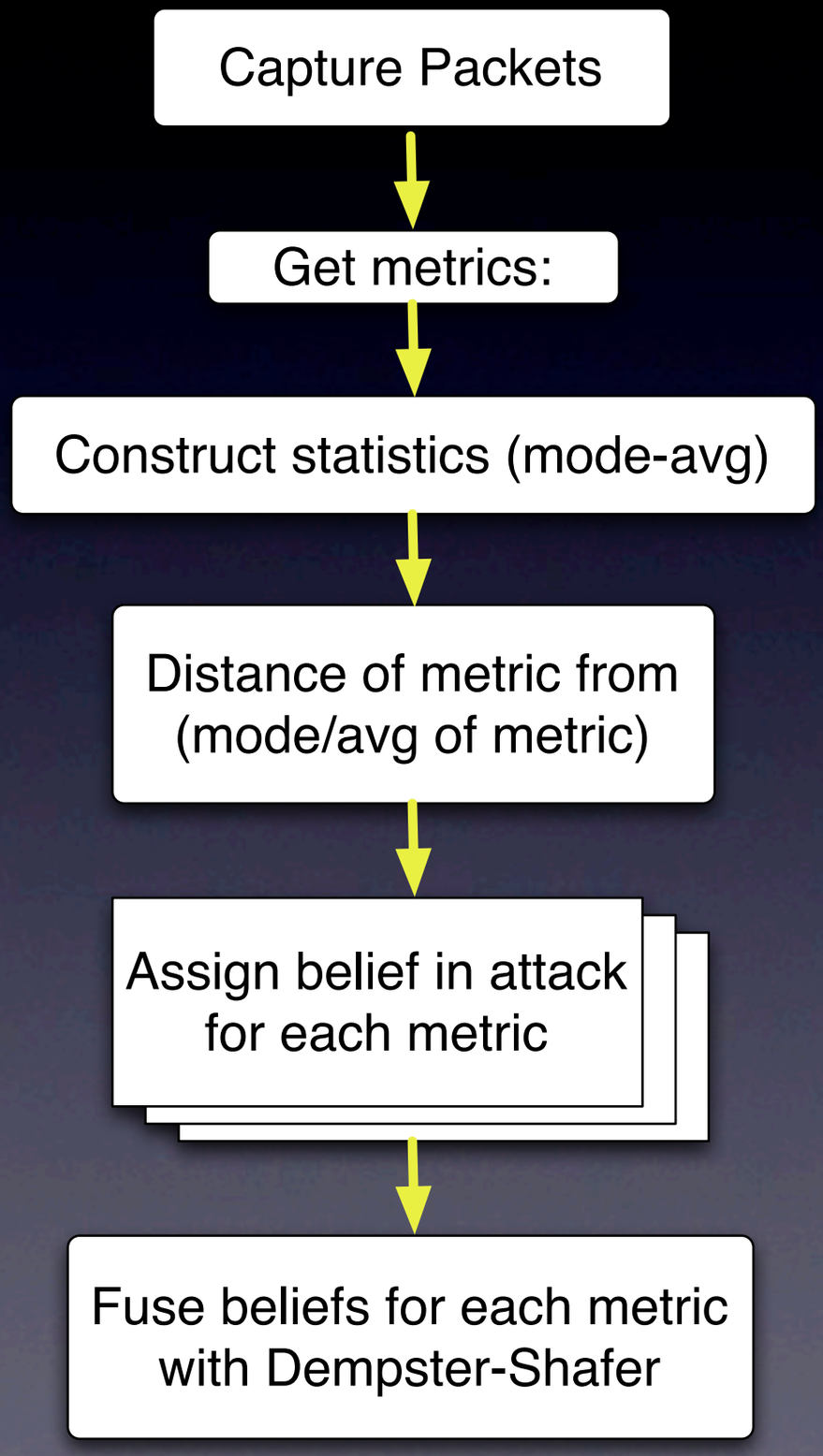
Wednesday, 6 July 2011

Metrics



- MAC Seq # : counter of frames from node
- NAV: Can be used as signature for node

Methodology



RSSI

RATE

TTL per flow

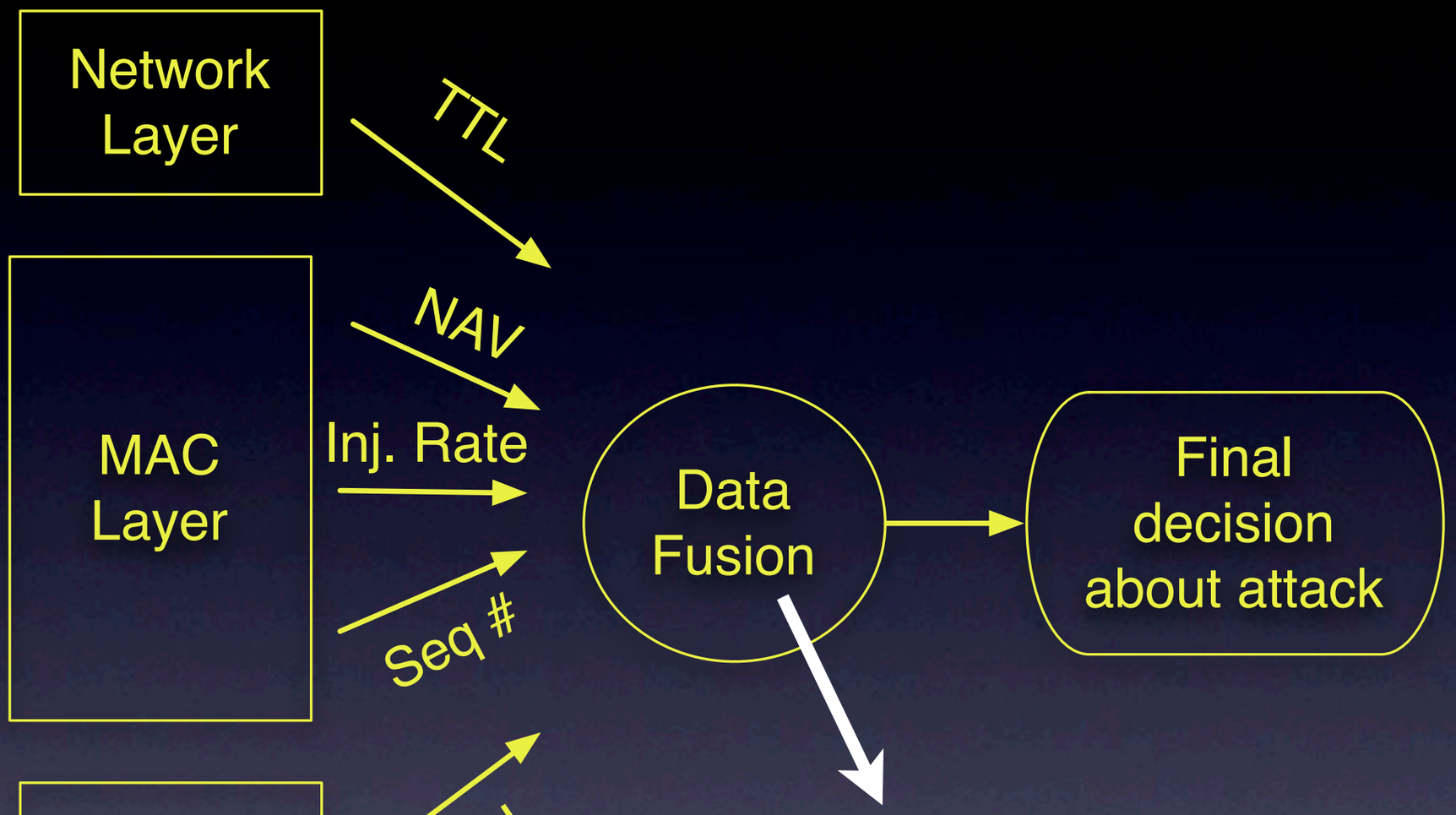
NAV

SEQ #

Most Volatile

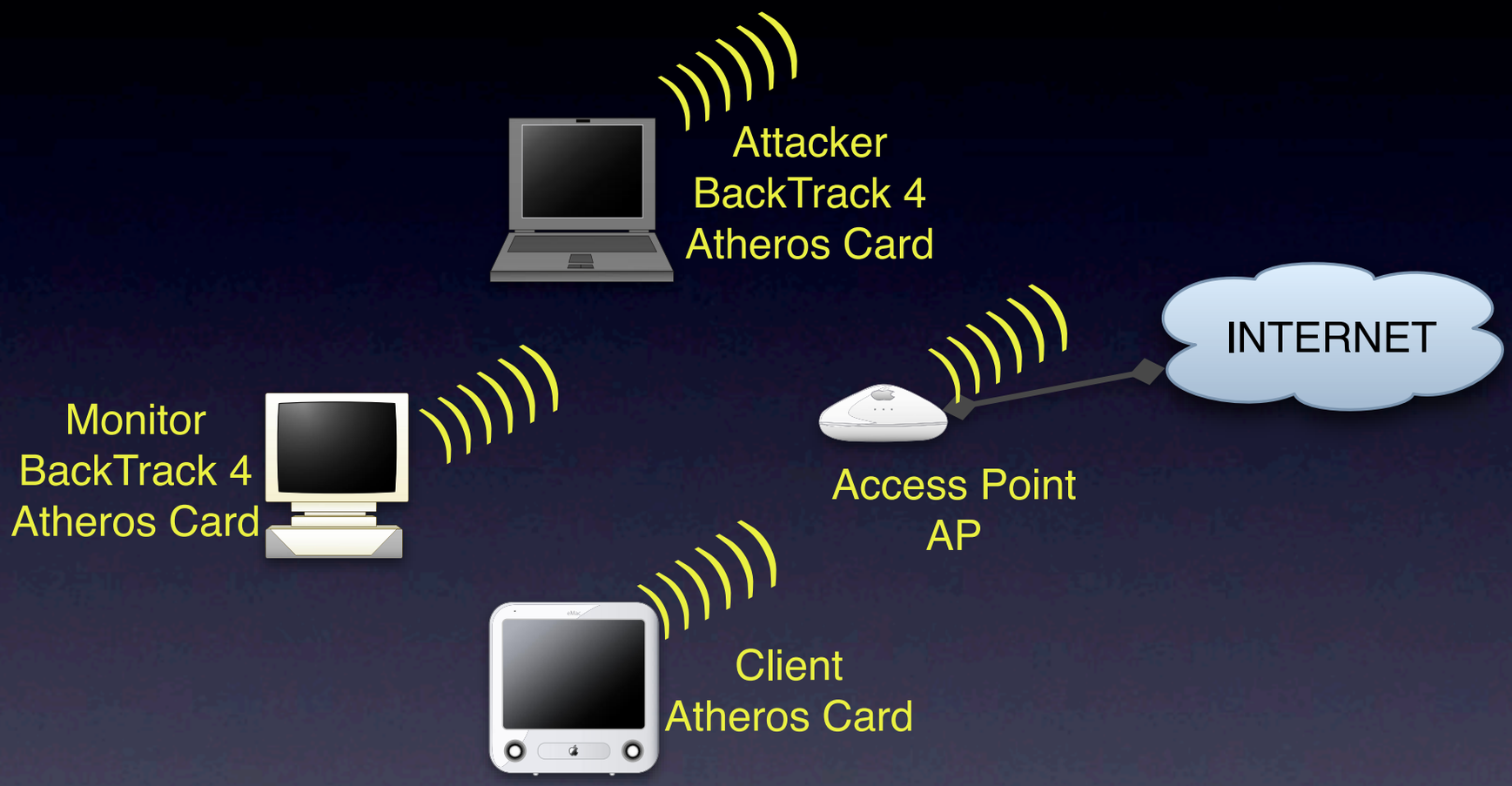
Least Volatile

Data Fusion

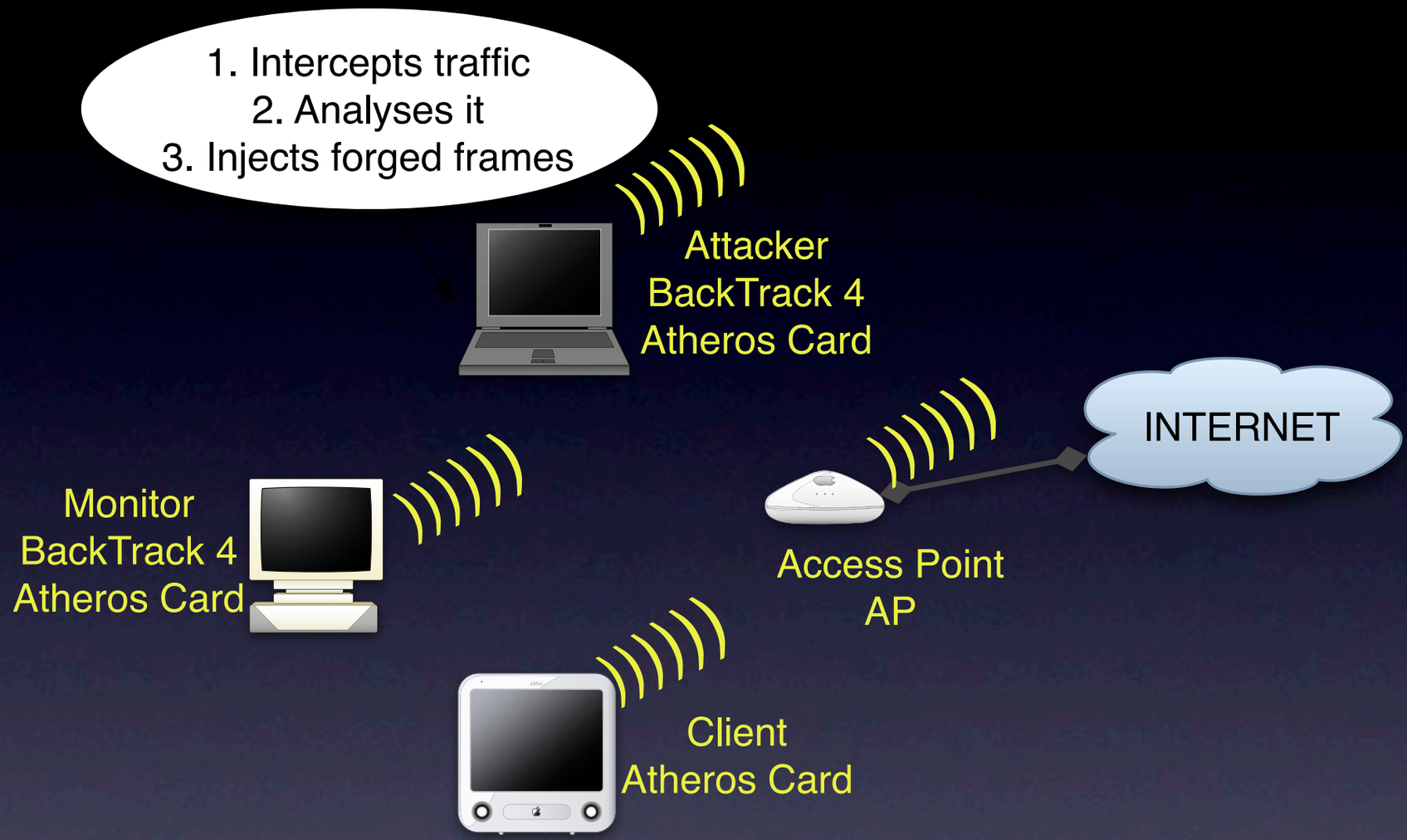


- ✳ Dempster-Shafer because:
  - Deals with uncertainty
  - No a priori knowledge

Test-bed


Attacker
BackTrack 4
Atheros Card
INTERNET
Monitor
BackTrack 4
Atheros Card
Access Point
AP
Client
Atheros Card

MitM Attack @ PHY

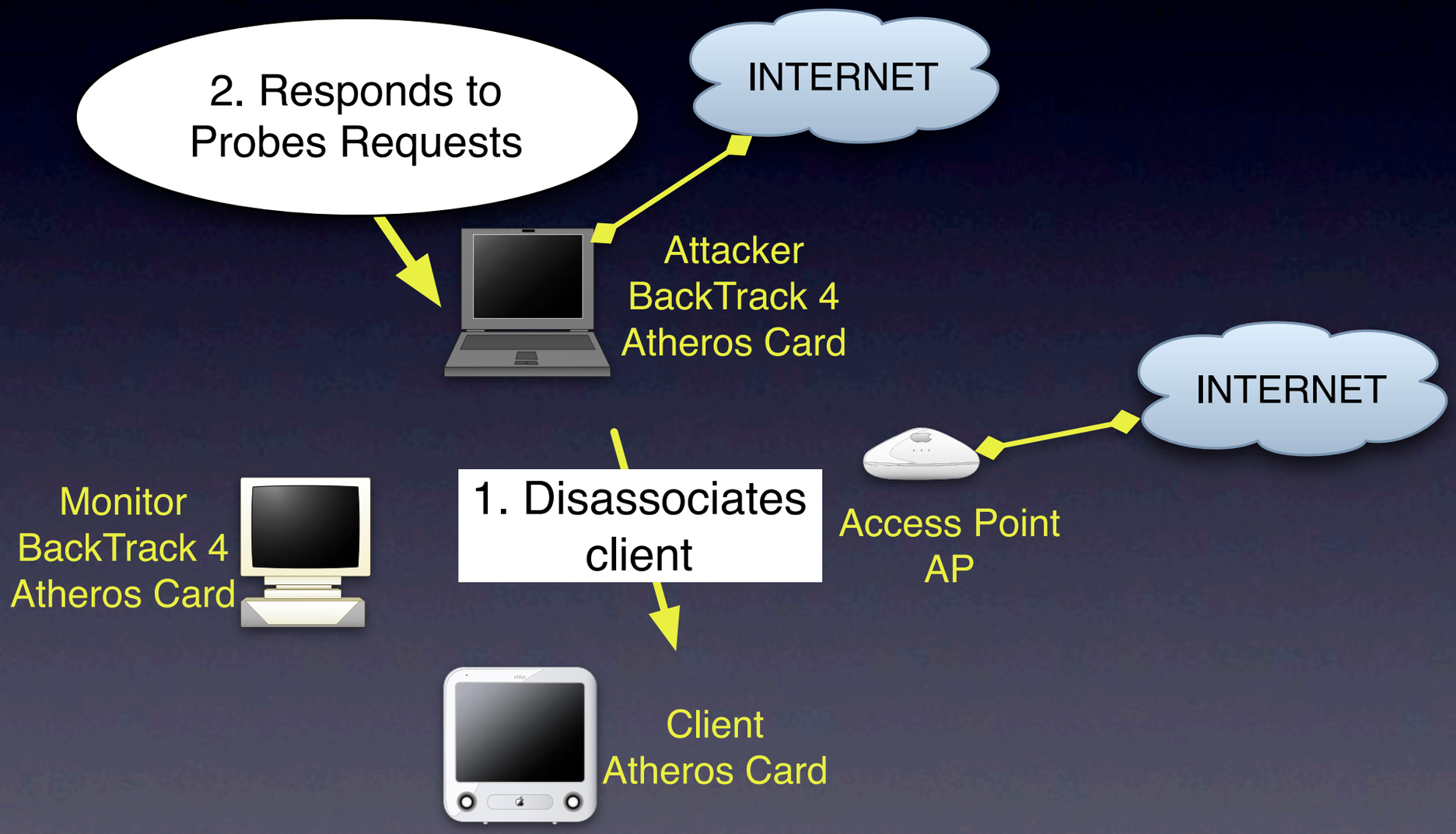


- Man in the Middle (MitM)
- Takes advantage of lag time
- Injects its own content

Results: MitM Attack

Metrics	Type	%	Result %
NAV + SEQ	FN	0	0
	FP	7/63	11.1
RSSI + NAV + SEQ	FN	0	0
	FP	8/63	12.7
RSSI + TTL + RATE	FN	0	0
	FP	0	0
All metrics	FN	0	0
	FP	0	0

Rogue AP attack



Rogue AP: Tools

Method	Rate	ESSID Spoof
Airbase	Fixed at 1Mbps	No
Airbase -a	Fixed at 1Mbps	Yes
Host AP	Normal Rate	No

Results: Rogue AP

Metrics	Type	Airbase	Airbase ESSID Spoof	HostAP
NAV + SEQ	Detected ?	Yes	Yes	Yes
	FP	0/405	0/246	0/57
RSSI + NAV + SEQ	Detected ?	Yes	Yes	Yes
	FP	35/405	2/246	3/57
RSSI + TTL + RATE	Detected ?	No	Yes	No
	FP	100%	0/246	100%
All metrics	Detected ?	Yes	Yes	Yes
	FP	0/405	0/246	0/57

Benefit of extra metrics

No. of Metrics	Beliefs		
	Attack	No Attack	Uncertainty
NAV-SEQ	0.569	0.314	0.118
RSSI - NAV - SEQ	0.664	0.263	0.073
RSSI - TTL - Rate	0.575	0.329	0.096
5 metrics	0.710	0.272	0.018

Benefit of extra metrics

- Benefit: Can adapt in case AP resets Seq # for valid reasons

Things to consider:

- Assume Normal traffic more than Attack
- Algorithm cleans polluted metrics from history given that several conditions apply:
  - If attack in NAV and if attack in SEQ # then remove last metrics from statistics

Conclusions

- ✳ Single metrics:
  - Inefficient, Inaccurate, Misleading
- ✳ Multi-metrics:
  - Synergistic Approach, More Accurate
- ✳ Data Fusion: Dempster-Shafer

Current and Future Work

- Automate assignment of beliefs
- Dynamic selection of metrics

Thank You ...