Who Is Peeping at Your Passwords at Starbucks?
– To Catch an Evil Twin Access Point

Yimin Song, **Chao Yang**, and Guofei Gu

Texas A&M University

Success Lab, Texas A&M University
July 1th, 2010

Pre-question

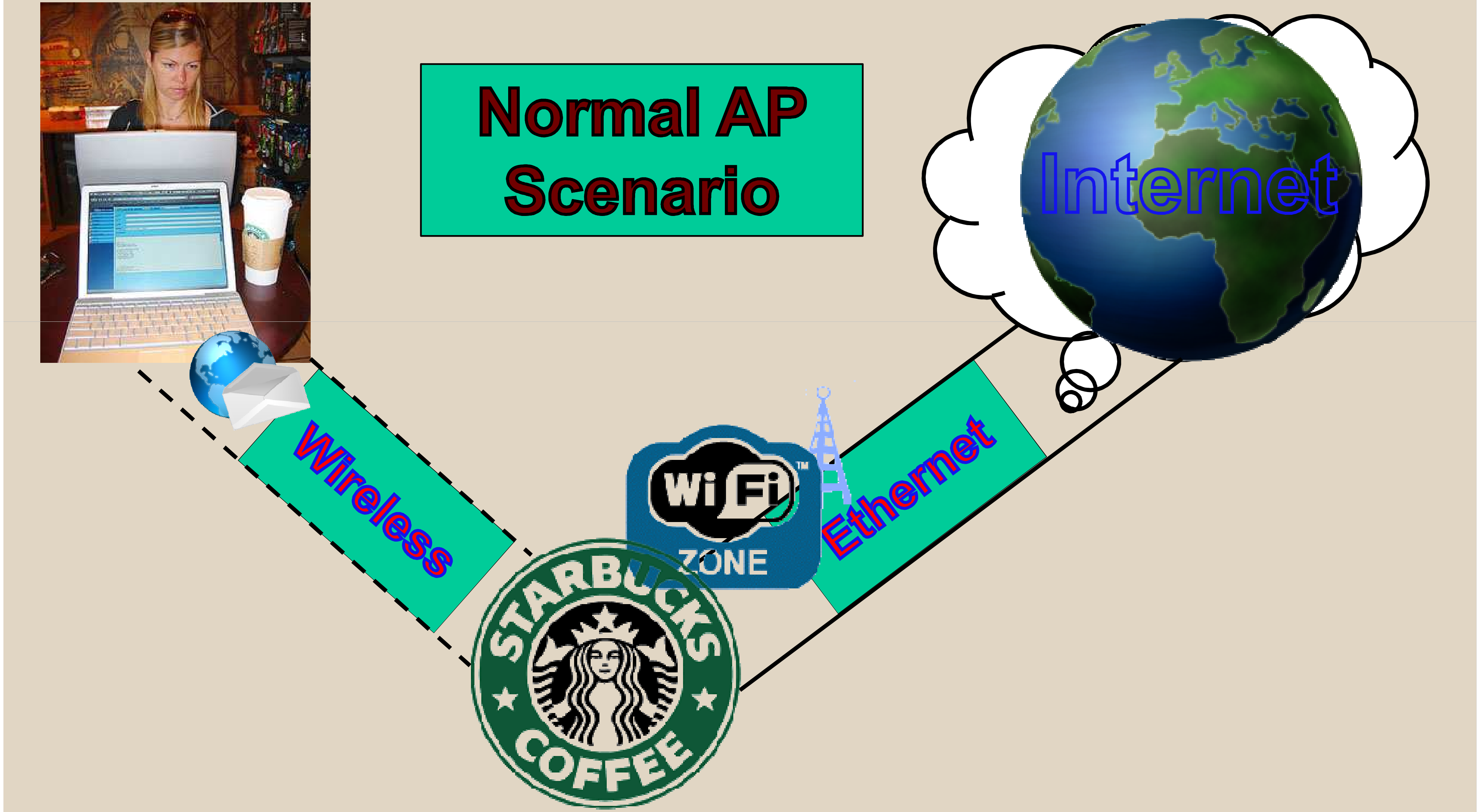
Evil Twin Attack!

Agenda

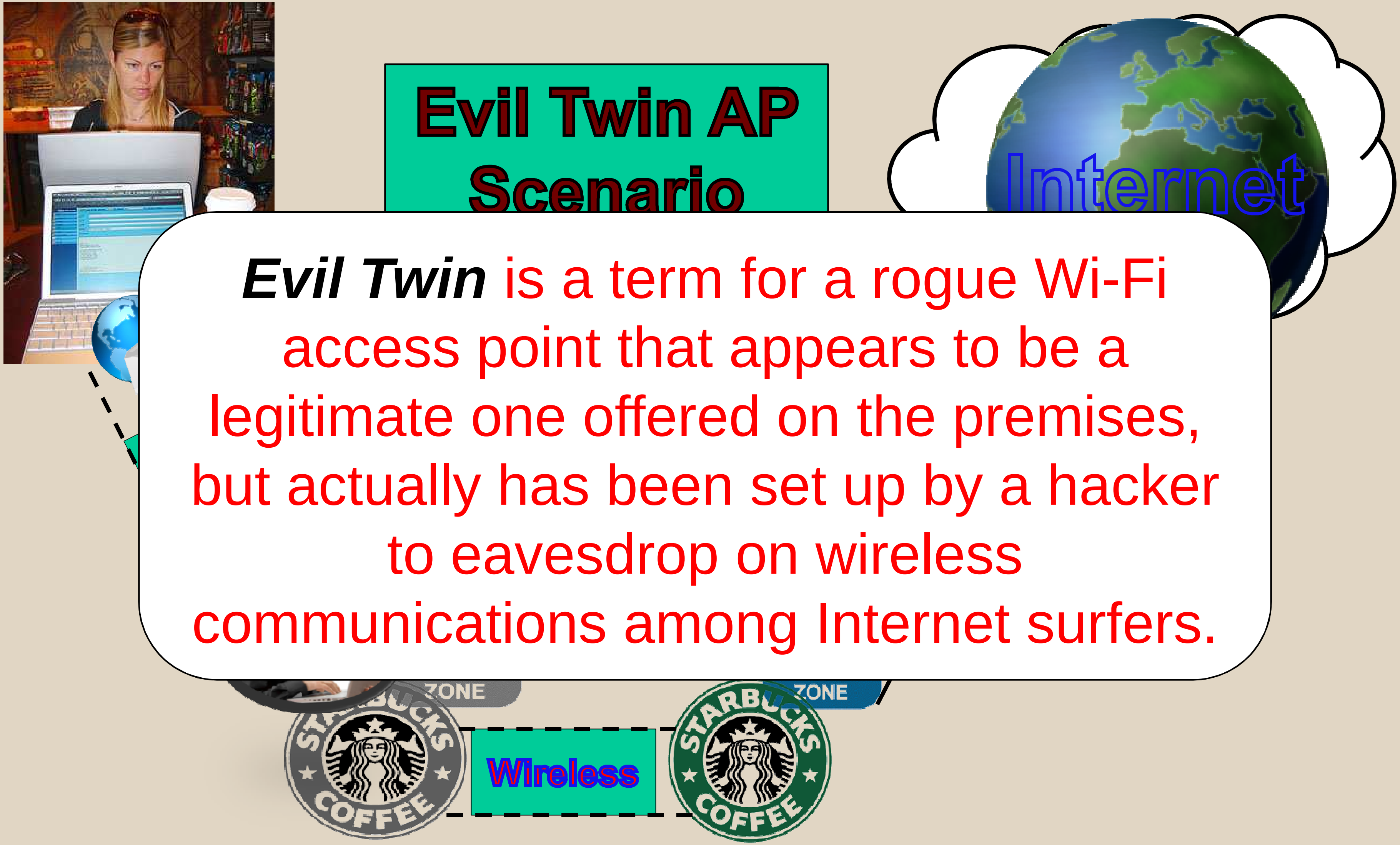
- Introduction
- ET-Sniffer
- Evaluation
- Summary & Future work

Introduction: Evil Twin Attack

Normal AP Scenario



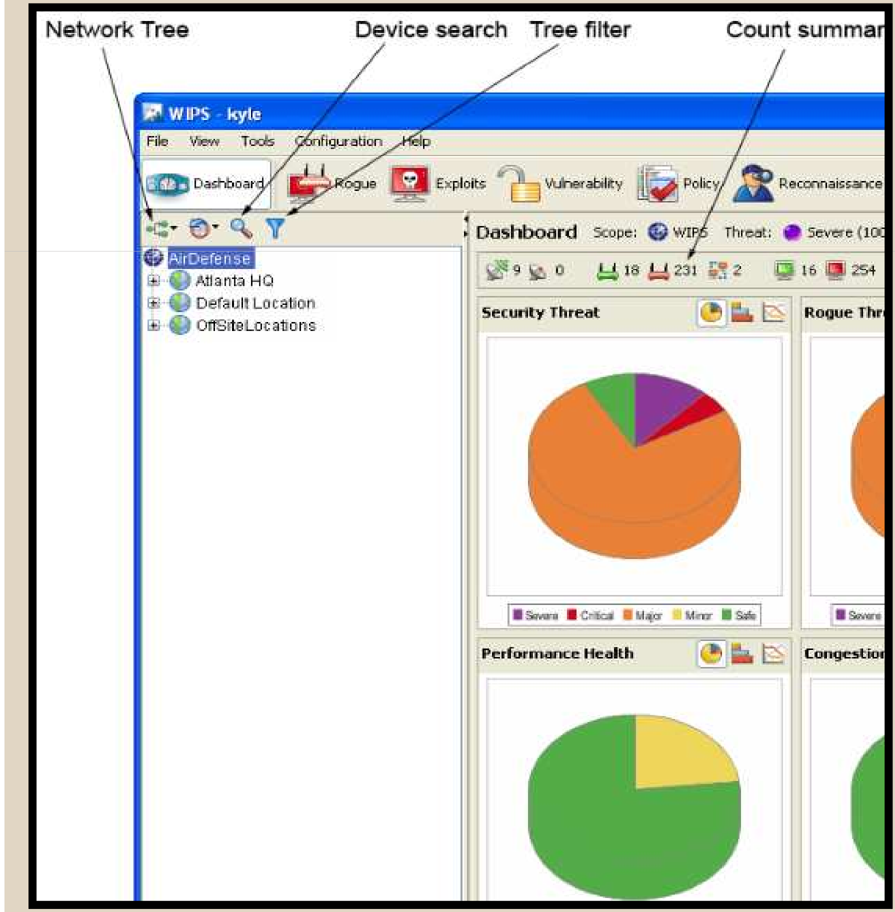
Introduction: Evil Twin Attack



Evil Twin is a term for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up by a hacker to eavesdrop on wireless communications among Internet surfers.

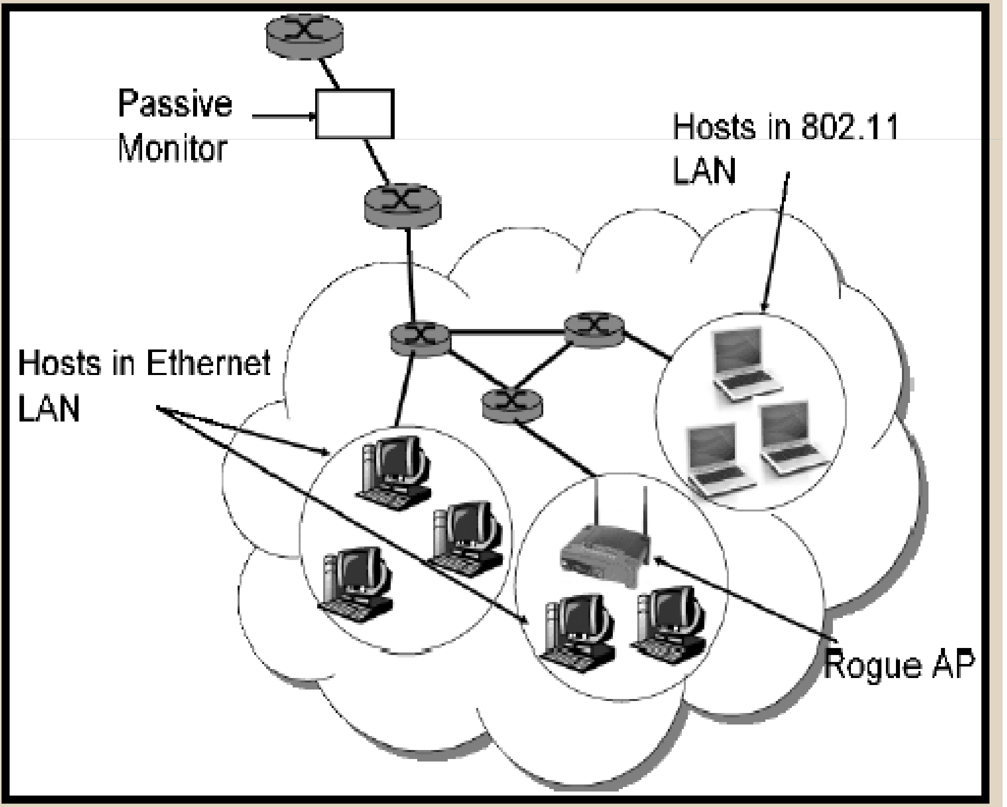
Introduction: Existing Methods For Detecting Rogue APs

AirDefense™

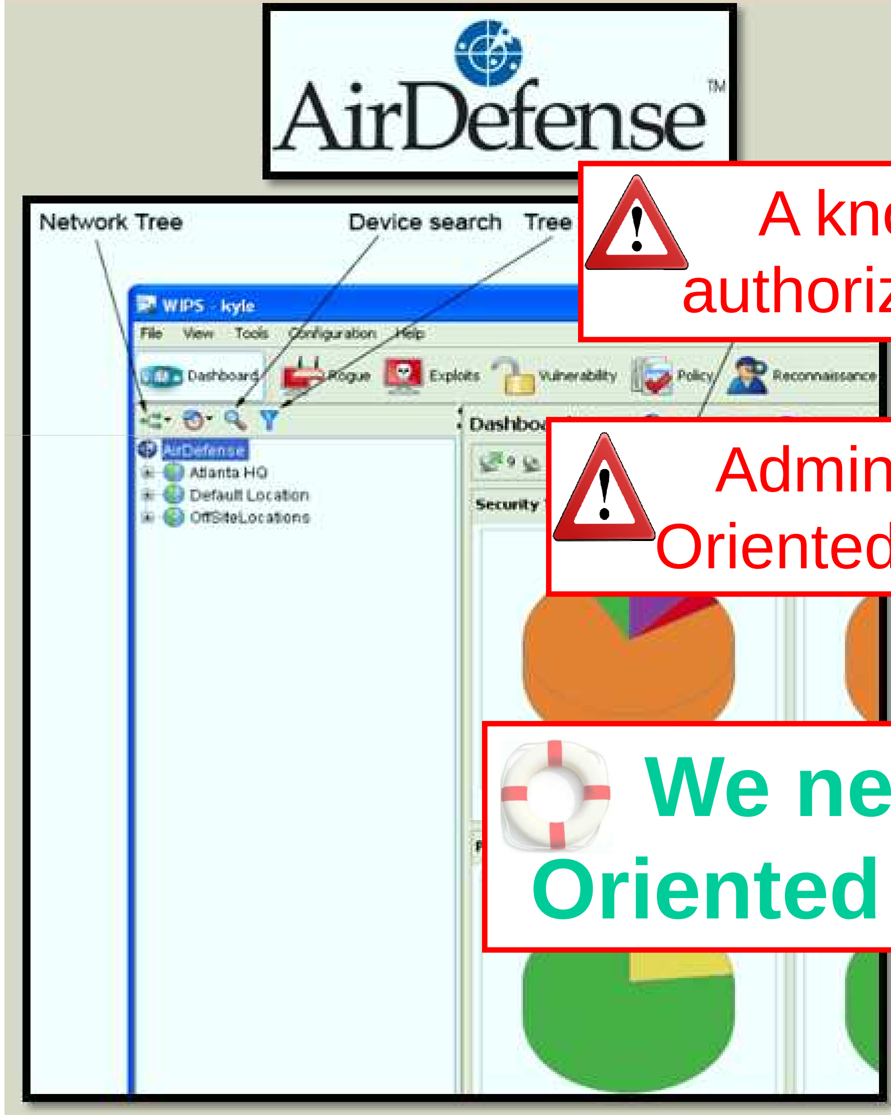


Wei, 2007

Passive Online Rogue Access Point Detection



Introduction: Existing Methods For Detecting Rogue APs



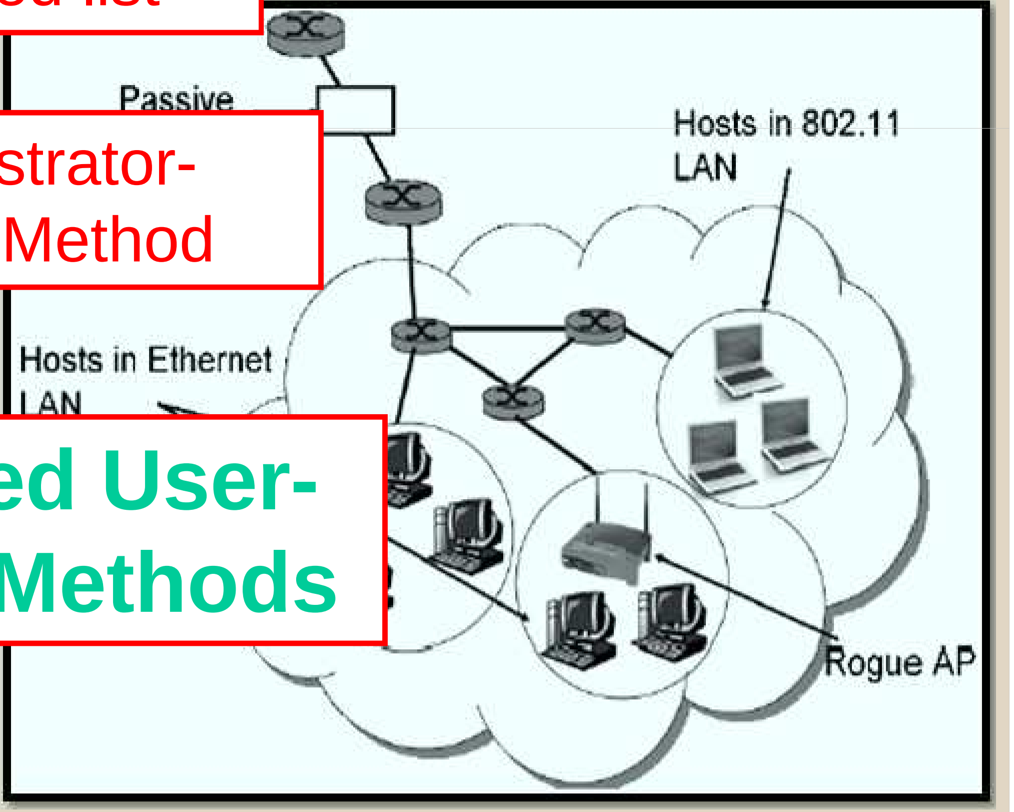
A known authorized list

Administrator-Oriented Method

We need User-Oriented Methods

Wei, 2007

Passive Online Rogue Access Point Detection



Introduction: *Characters of ET-Sniffer(Evil Twin Sniffer)*

- Light-weight
- User side
- Active detection
- Needless to keep an authorized list
- High detection rate
- Low false positive rate

Agenda

- Introduction
- **ET-Sniffer**
- Evaluation
- Summary & Future work

ET-Sniffer: *Attack Model*

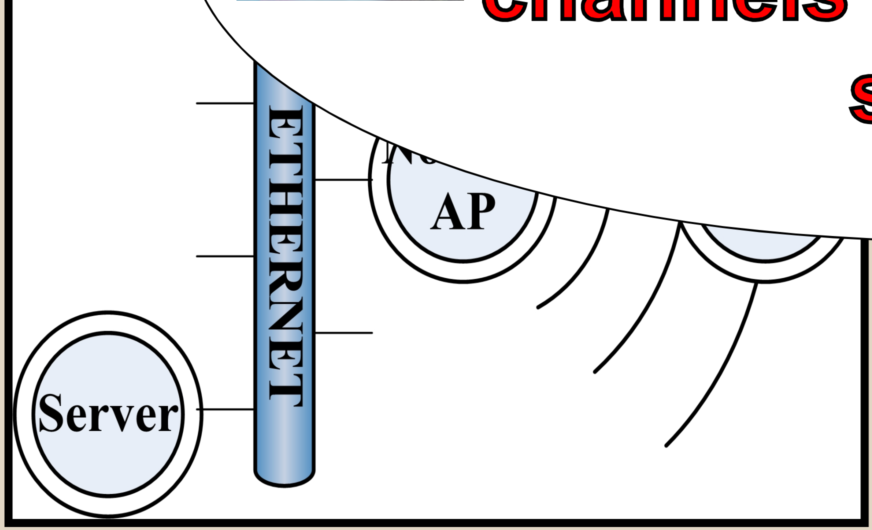
Normal AP Scenario

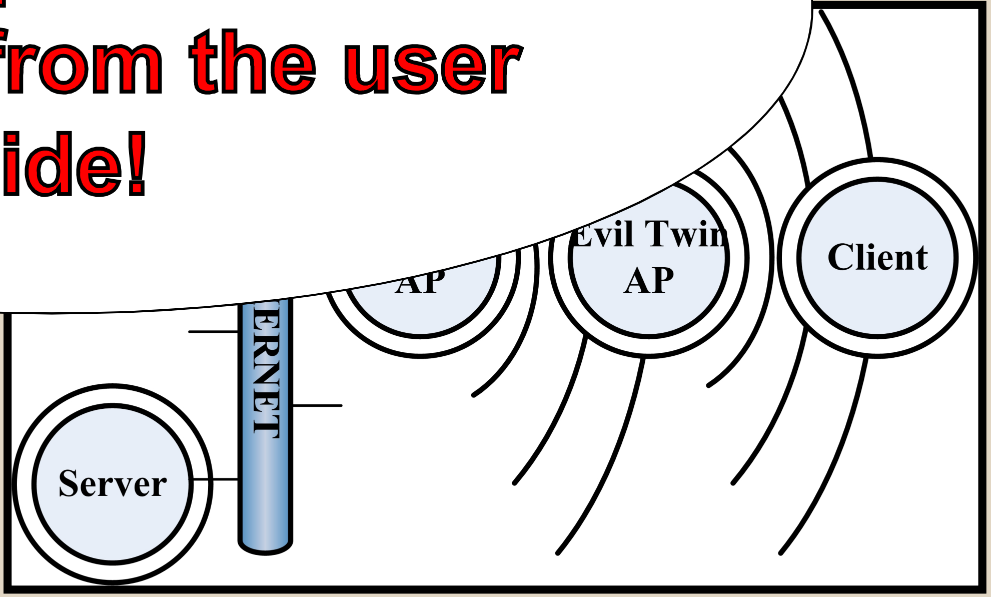
Evil Twin AP Scenario

One-ho

reless

Differentiate one-hop and two-hop wireless channels from the user side!





ET-Sniffer: *Questions to be considered*

- What ***statistics*** can be used to effectively distinguish on nd two-hop wireless channels c
- Are there a ***amic facto*** l network en n statistics?
- How to de nt ***detection algorithms*** with the conside influencing facto

ter-packet Arrival Time (IAT)

RSSI ↓

IAT ↑

Received Signal Strength In)

Wireless saturation

Saturation ↑

IAT ↑

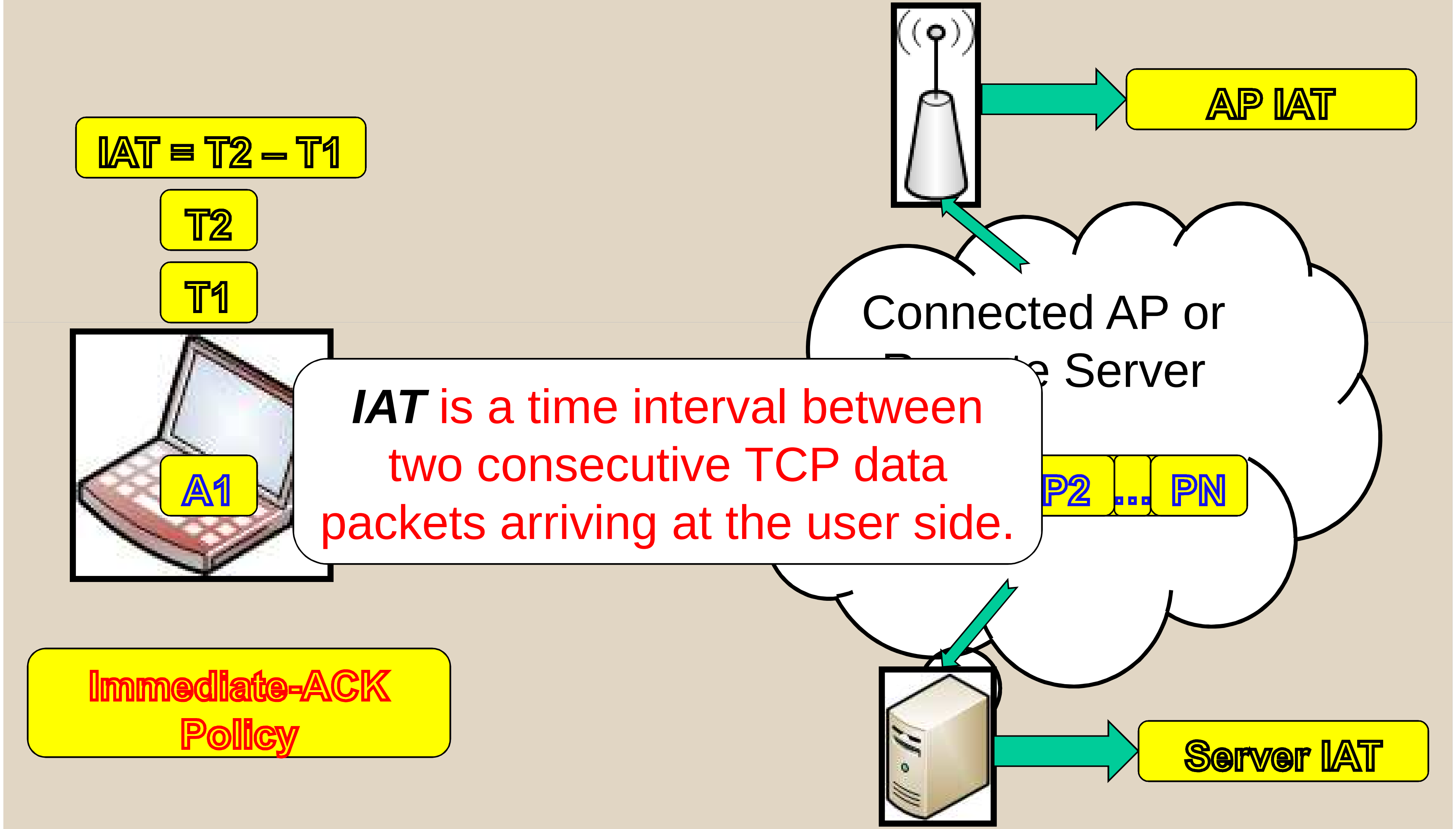
Need to train a model using pre-collected packets

Does not need to train a model

Trained Mean Matching (TMM)

Hop Differentiating Technique (HDT)

ET-Sniffer: *IAT*

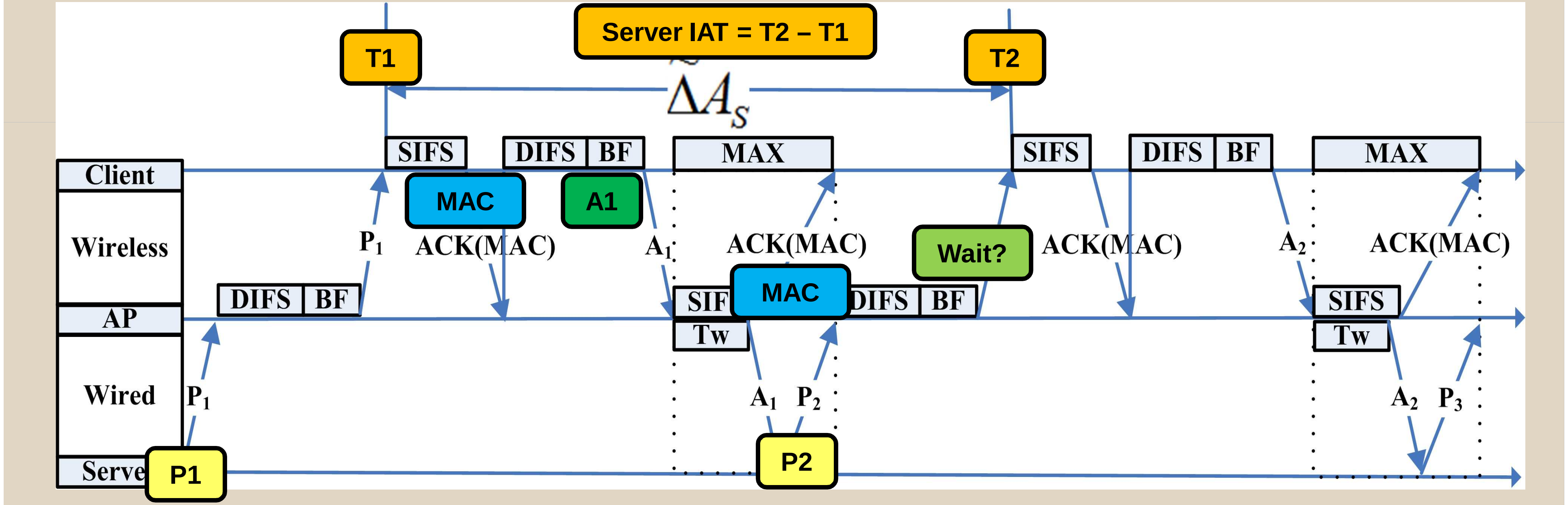


IAT is a time interval between two consecutive TCP data packets arriving at the user side.

Immediate-ACK Policy

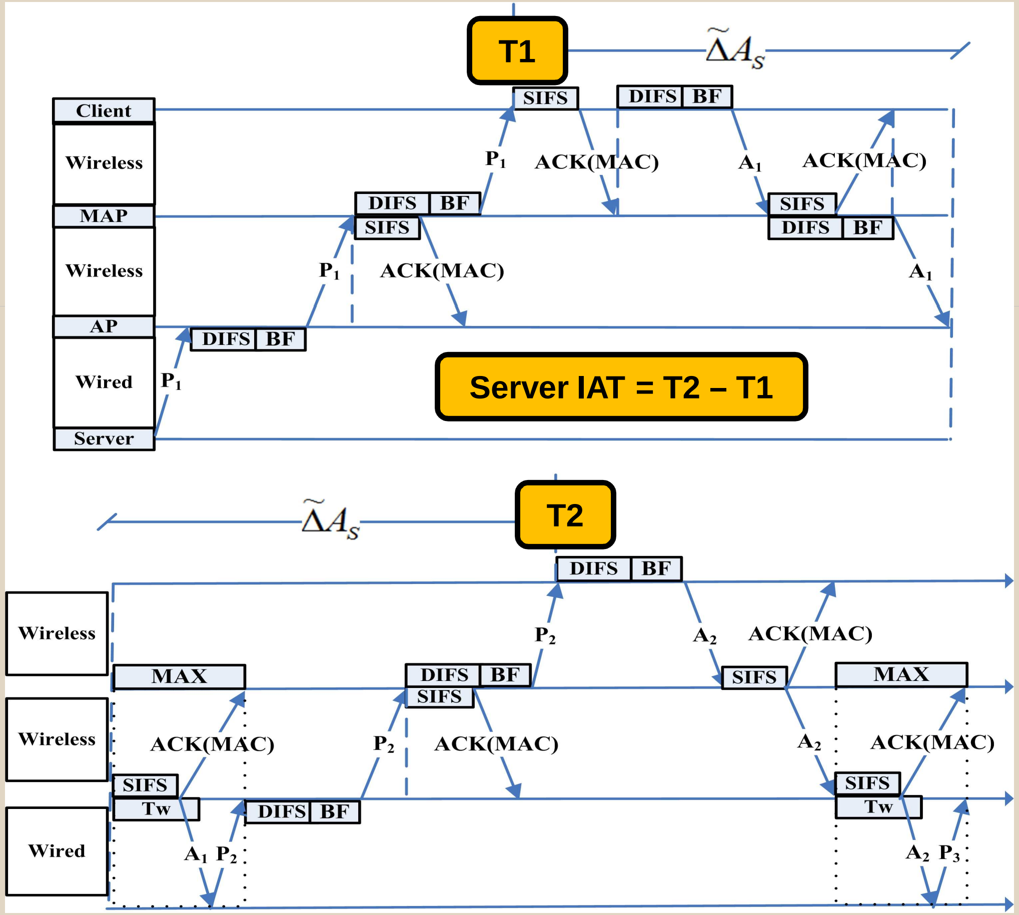
ET-Sniffer: *Trained Mean Match—Server IAT Calculation*

Normal AP Scenario



ET-Sniffer: *Trained Mean Match—Server IAT Calculate*

Evil Twin AP Scenario



ET-Sniffer: *Trained Mean Match—Server IAT Calculation*

$$E(\Delta_S) = E(\Delta A_S)_{two-hop} - E(\Delta A_S)_{one-hop} \approx E(\tilde{\Delta}_S)$$
$$= 2T_{DIFS} + 2E(T_{BF}) + \frac{L_{ACK(TCP)} + L_P}{B_W}$$

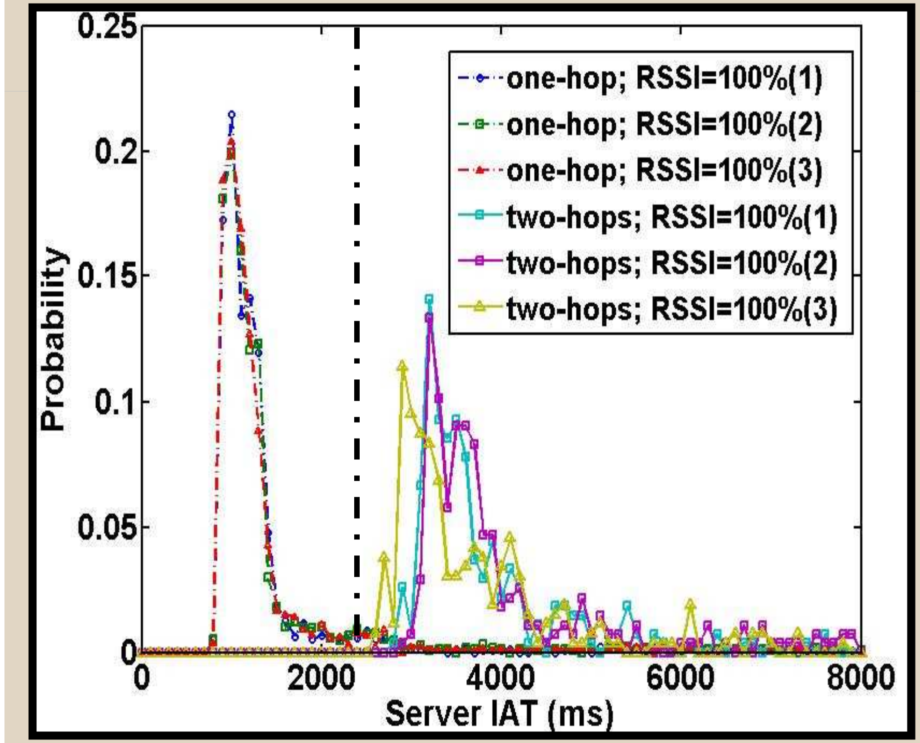
An obvious gap of the Server IAT in the two scenarios.

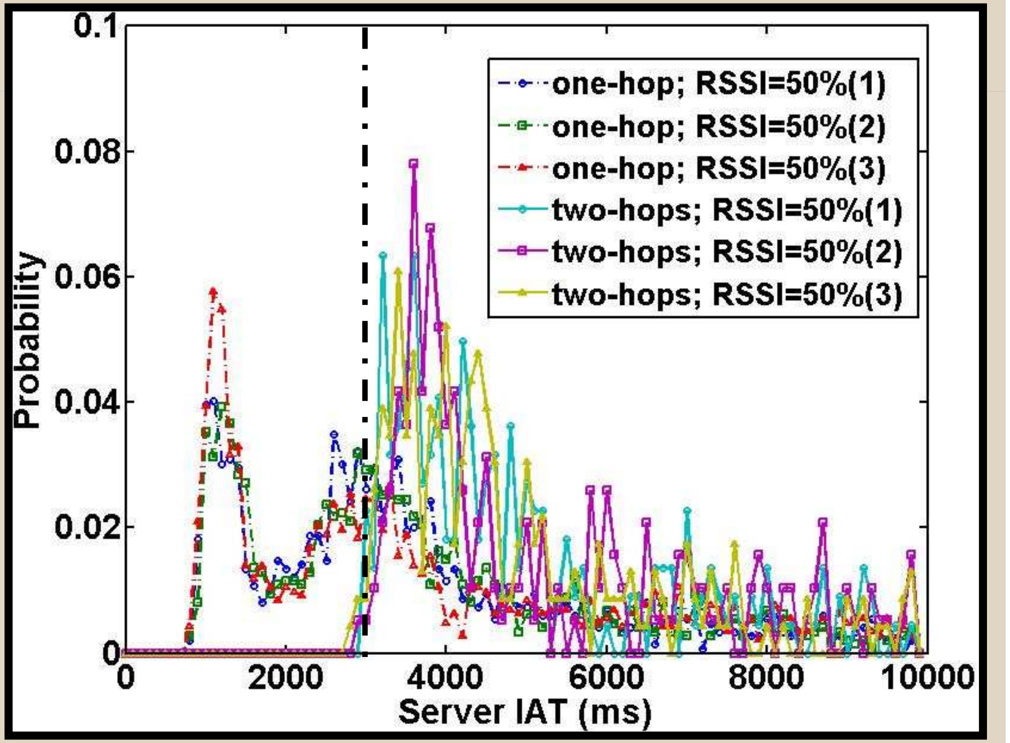
This observation can be used to detect an evil twin attack!

ET-Sniffer: *Trained Mean Match--Practical validation*

RSSI = 100%

RSSi = 50%





ET-Sniffer: *Trained Mean Match--Algorithm*

- Training Phase: a quadratic-mean technique to train a detection threshold
- Detecting Phase: accumulate the degree of suspicion -- Sequential Probability Ratio Test (SPRT)
  - At each round, collect a server IAT and compute a likelihood ratio to be an evil twin attack.
  - Accumulate the sum of the likelihood.
  - After several rounds, make the decision when the sum attains the bound.

ET-Sniffer: *Trained Mean Match--Discussion*

- Training & Detecting Method: Need to pre-collect network packets to train a threshold to detect
  - Time
  - Location
  - Network
- Motivate us to design an algorithm without the need of training a threshold

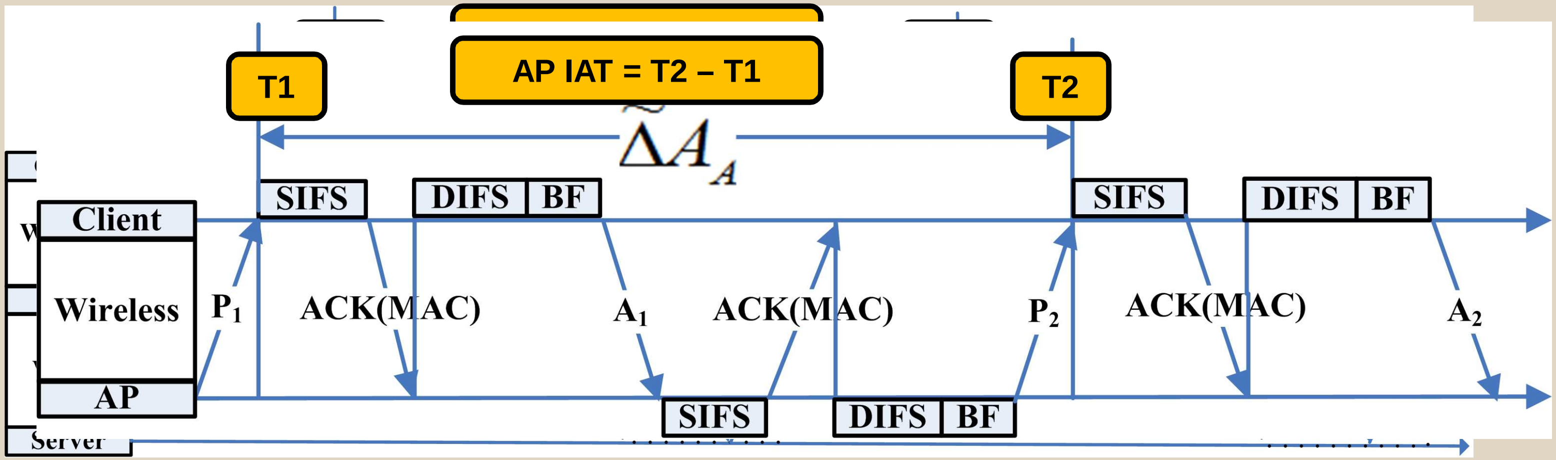
ET-Sniffer: *Hop Differentiate Technique*

- Does not need to train!
- Use another detection parameter so that we can obtain a relatively constant threshold to detect
- Server-to-AP IAT Ratio (SAIR): The ratio of a Server IAT to an AP IAT

ET-Sniffer: *Hop Differentiate Technique--SAIR*

Normal AP Scenario

SAIR ← Server IAT ÷ AP IAT



ET-Sniffer: *Hop Differentiate Technique--SAIR*

- In 802.11b, the mean of SAIR in one-hop wireless channel is smaller than 1.00; the mean of SAIR in two-hop wireless channel is bigger than 1.74.
- In 802.11g, the mean of SAIR in one-hop wireless channel is smaller than 1.11; the mean of SAIR in two-hop wireless channel is bigger than 1.94.

ET-Sniffer: *HDT--Threshold setting and detecting*

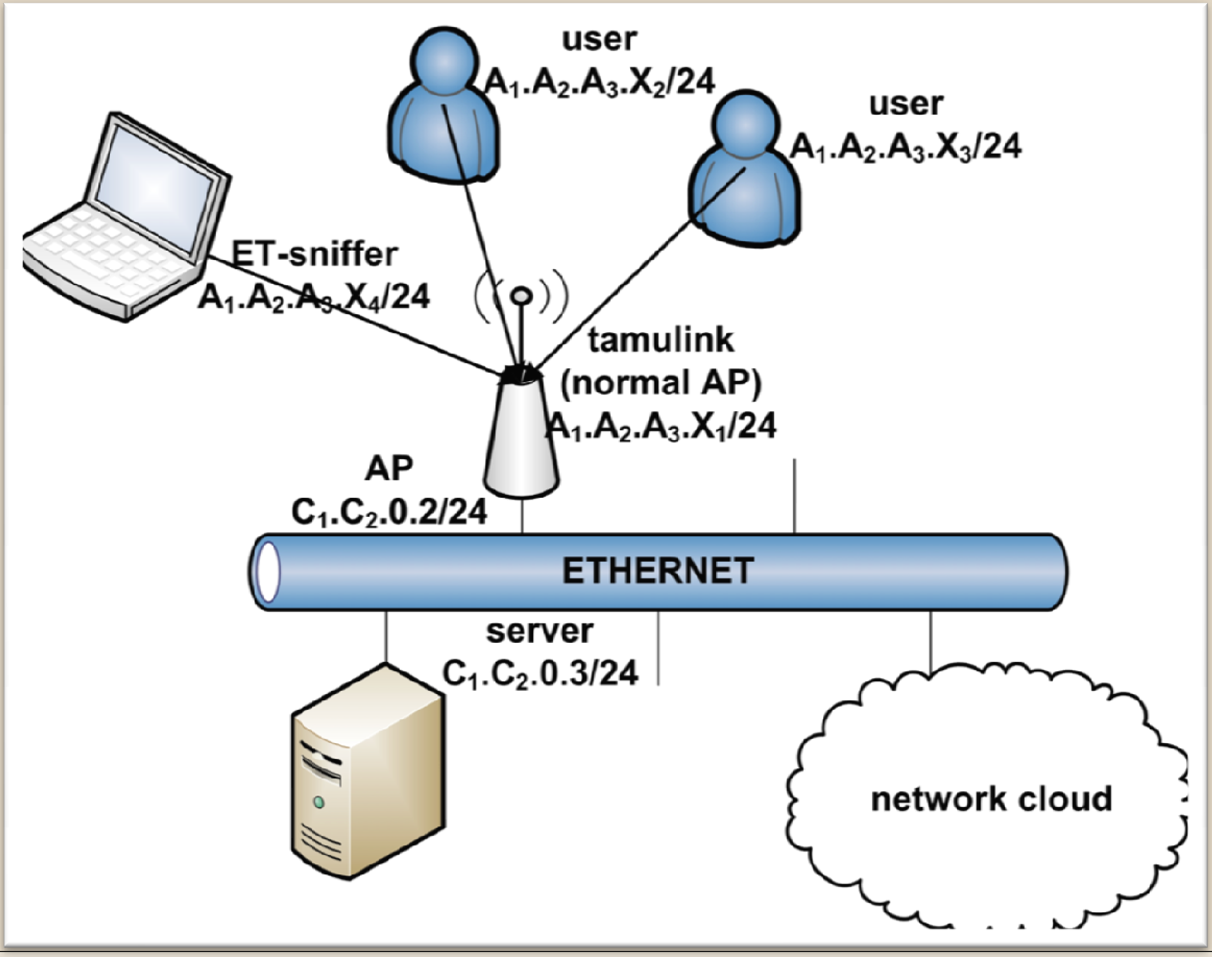
- Threshold Setting:
  - The threshold interval: $\alpha_\theta \in [1, 2]$
  - Minimize the probability of making wrong decision
  - For 802.11b, $\alpha_\theta = 1.34$
  - For 802.11g, $\alpha_\theta = 1.48$
- Detecting: SPRT

Agenda

- Introduction
- ET-Sniffer
- **Evaluation**
- Summary & Future work

Evaluation: *Experimental setup- -Normal AP Scenario*

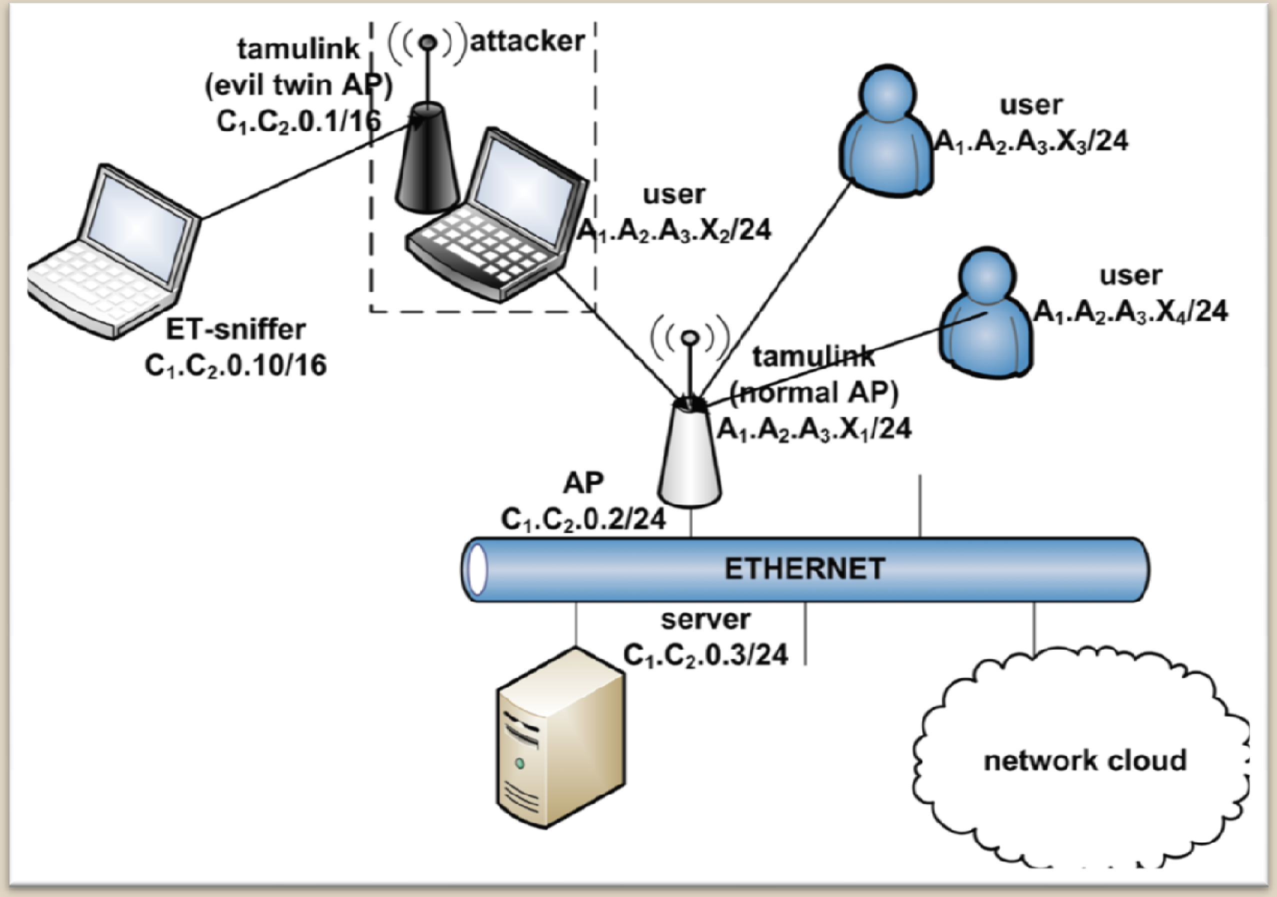
Normal AP Scenario



Evaluation: Experimental setup--Evil Twin AP Scenario

TEXAS A&M UNIVERSITY

Evil Twin AP Scenario



Evaluation: *Effectiveness*

RSSI Ranges

Range	A	B+	B-	C+	C-	D	E
Upper	100%	80%	70%	60%	50%	40%	20%
Lower	80%	70%	60%	50%	40%	20%	0%

Detection Rate

RSSI Range	A	B+	B-	C+	C-	D
802.11g(TMM)	99.39%	99.97%	99.49%	99.50%	98.32%	94.36%
802.11b(TMM)	99.81%	95.43%	94.81%	96.09%	91.94%	85.71%
802.11g(HDT)	99.08%	98.72%	93.53%	94.31%	87.29%	81.39%
802.11b(HDT)	99.92%	99.99%	99.96%	99.95%	96.05%	94.64%

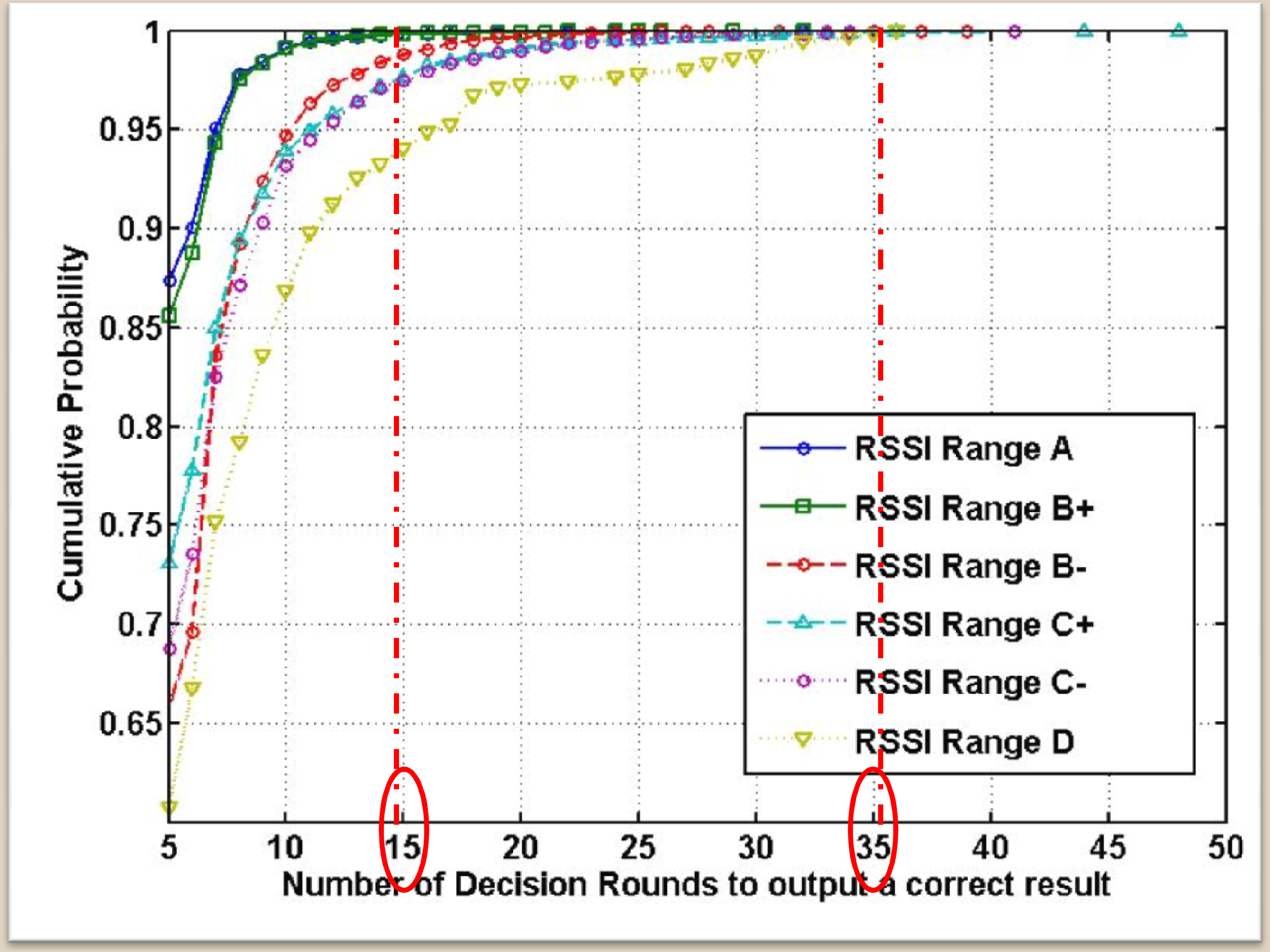
Evaluation: *Effectiveness--Multi-packets*

- Use the mean of multiple Server IATs and the mean of multiple SAIRs in one decision round in the detection phase.

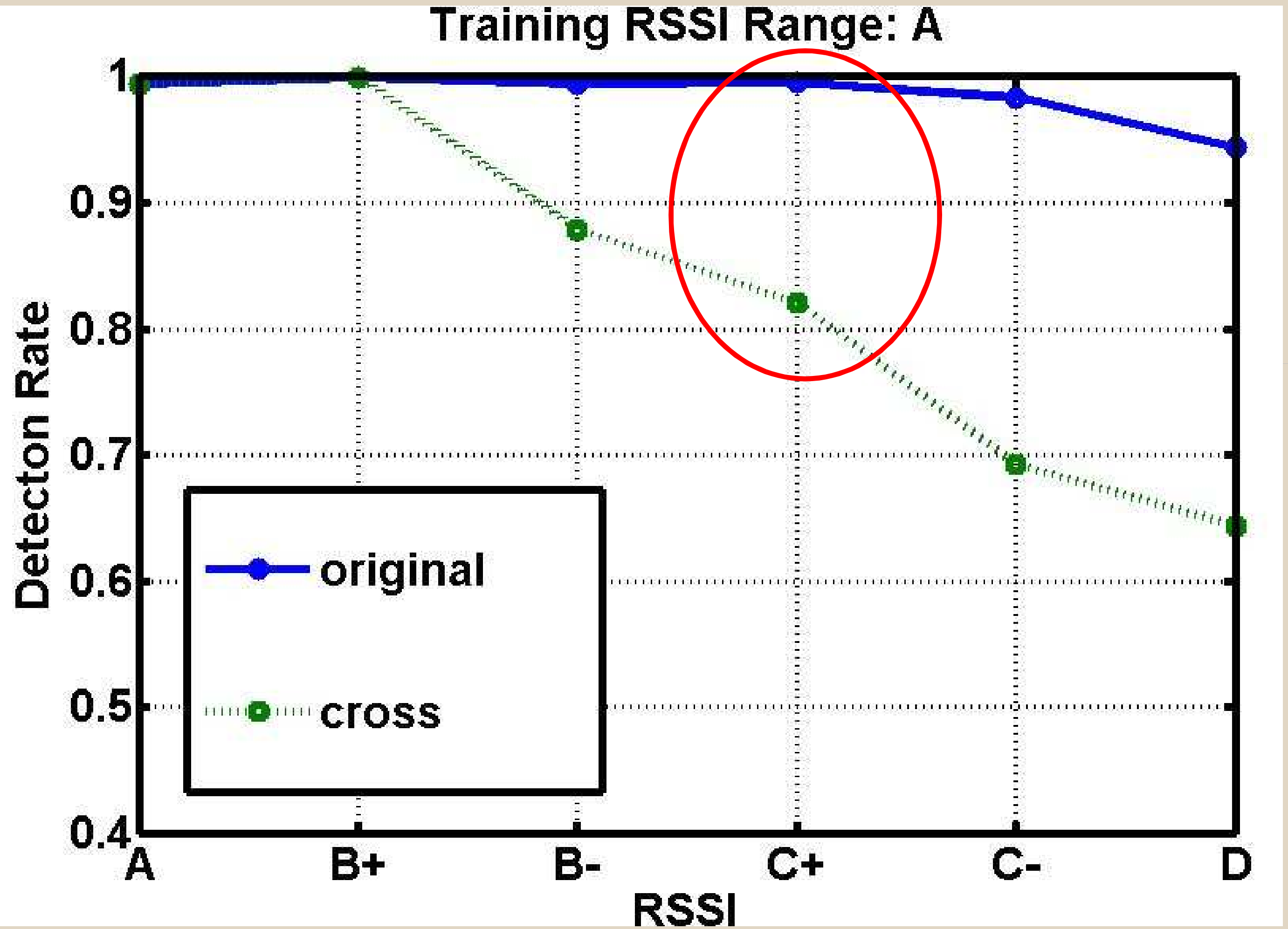
Detection Rate(50)

RSSI Range	A	B+	B-	C+	C-	D
802.11g(multi-TMM)	99.62%	100%	100%	99.95%	100%	100%
802.11b(multi-TMM)	100%	100%	100%	100%	100%	100%
802.11g(multi-HDT)	100%	99.11%	98.73%	99.88%	95.83%	88%
802.11b(multi-HDT)	100%	100%	100%	100%	100%	100%

Evaluation: *Time Efficiency*

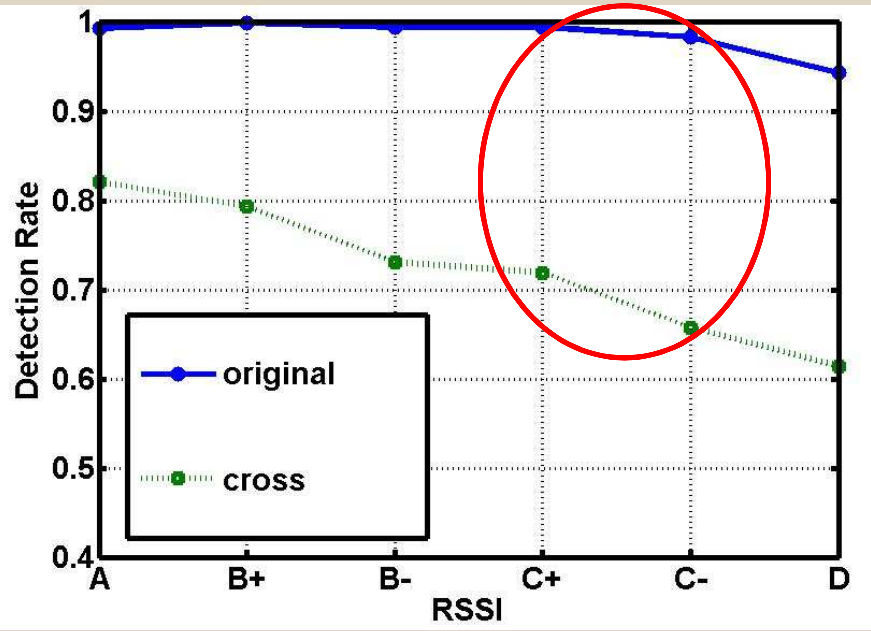


Evaluation: *Cross-validation-- under different RSSI for TMM*

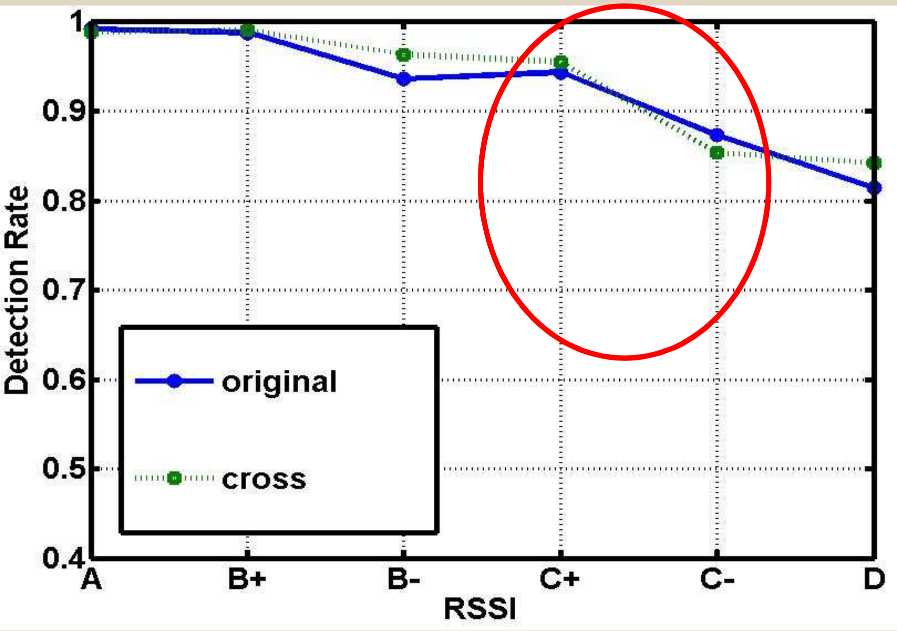


Evaluation: *Cross-validation-- under different locations*

TMM



HDT



Agenda

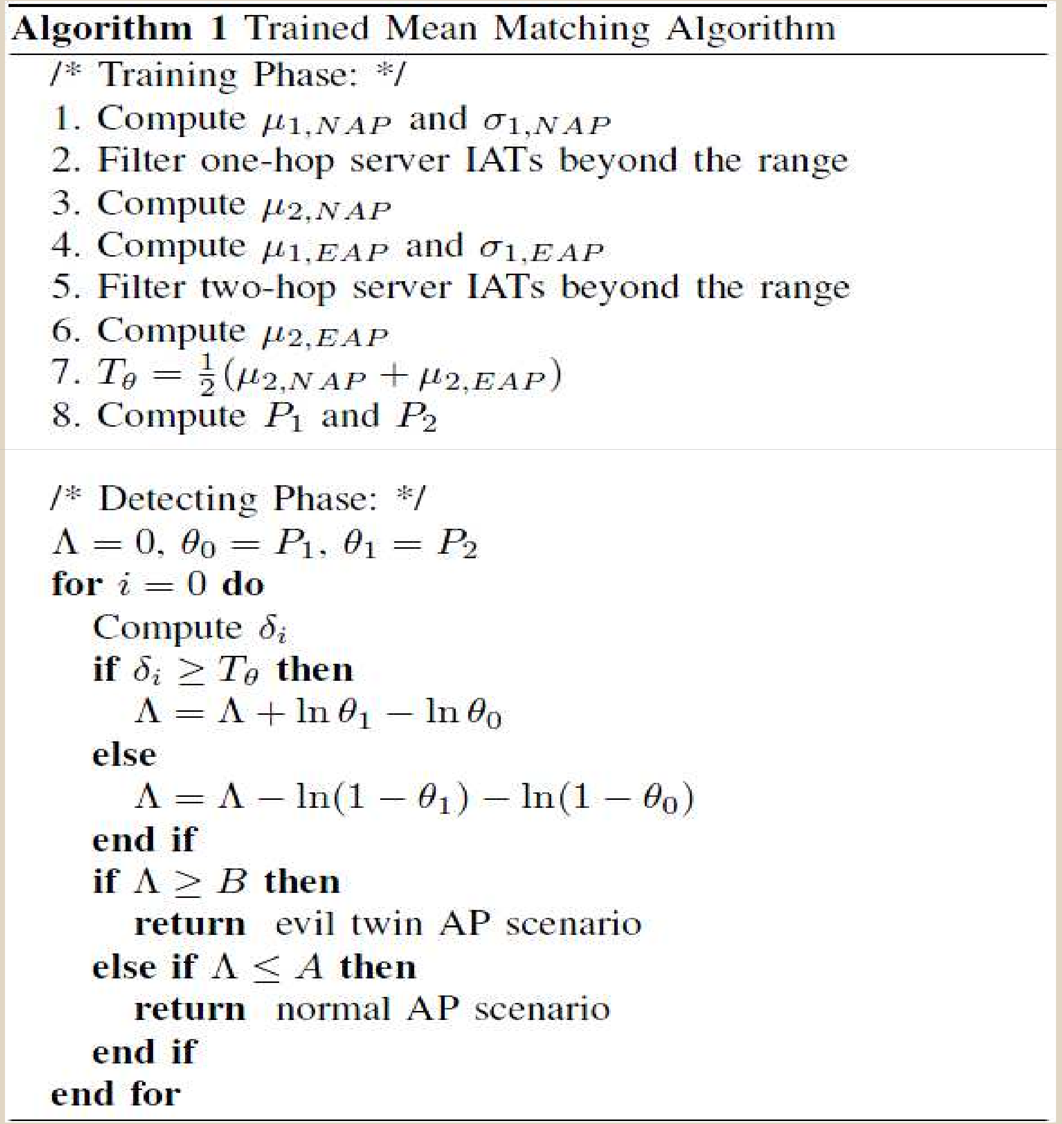
- Introduction
- ET-Sniffer
- Evaluation
- **Summary & Future work**

Summary & Future Work

- Summary
  - The first user-side evil twin detection solution
  - Design two detection algorithms
  - A prototype system, ET-Sniffer, which is effective and time efficient
- Future Work
  - A general malicious AP detection: e.g. a malicious AP may not require the normal AP to relay traffic

Questions & Answers

ET-Sniffer: *TMM--Algorithm*



Algorithm 1 Trained Mean Matching Algorithm

```
/* Training Phase: */
1. Compute $\mu_{1,NAP}$ and $\sigma_{1,NAP}$
2. Filter one-hop server IATs beyond the range
3. Compute $\mu_{2,NAP}$
4. Compute $\mu_{1,EAP}$ and $\sigma_{1,EAP}$
5. Filter two-hop server IATs beyond the range
6. Compute $\mu_{2,EAP}$
7. $T_\theta = \frac{1}{2}(\mu_{2,NAP} + \mu_{2,EAP})$
8. Compute $P_1$ and $P_2$

/* Detecting Phase: */
$\Lambda = 0$, $\theta_0 = P_1$, $\theta_1 = P_2$
for $i = 0$ do
  Compute $\delta_i$
  if $\delta_i \geq T_\theta$ then
    $\Lambda = \Lambda + \ln \theta_1 - \ln \theta_0$
  else
    $\Lambda = \Lambda - \ln(1 - \theta_1) - \ln(1 - \theta_0)$
  end if
  if $\Lambda \geq B$ then
    return evil twin AP scenario
  else if $\Lambda \leq A$ then
    return normal AP scenario
  end if
end for
```

Evaluation: *Effectiveness*

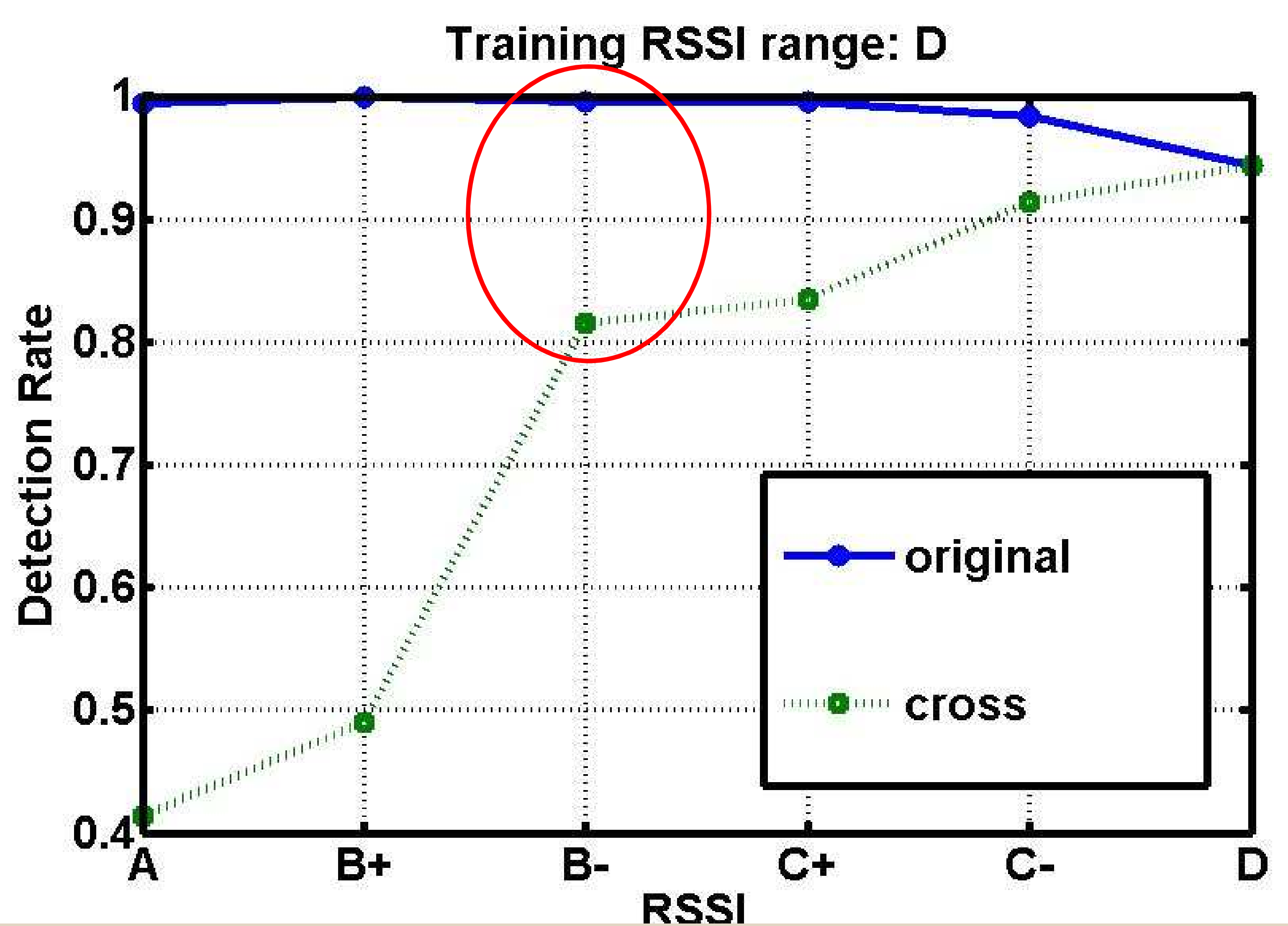
False Positive Rate

RSSI	A	B+	B-	C+	C-	D
802.11g(TMM)	1.08%	1.76%	1.97%	1.48%	1.75%	1.73%
802.11b(TMM)	0.78%	1.00%	1.07%	1.27%	6.65%	7.01%
802.11g(HDT)	2.19%	1.41%	2.06%	1.93%	2.48%	6.52%
802.11b(HDT)	8.39%	8.76%	5.39%	6.96%	5.27%	5.15%

False Positive Rate(50)

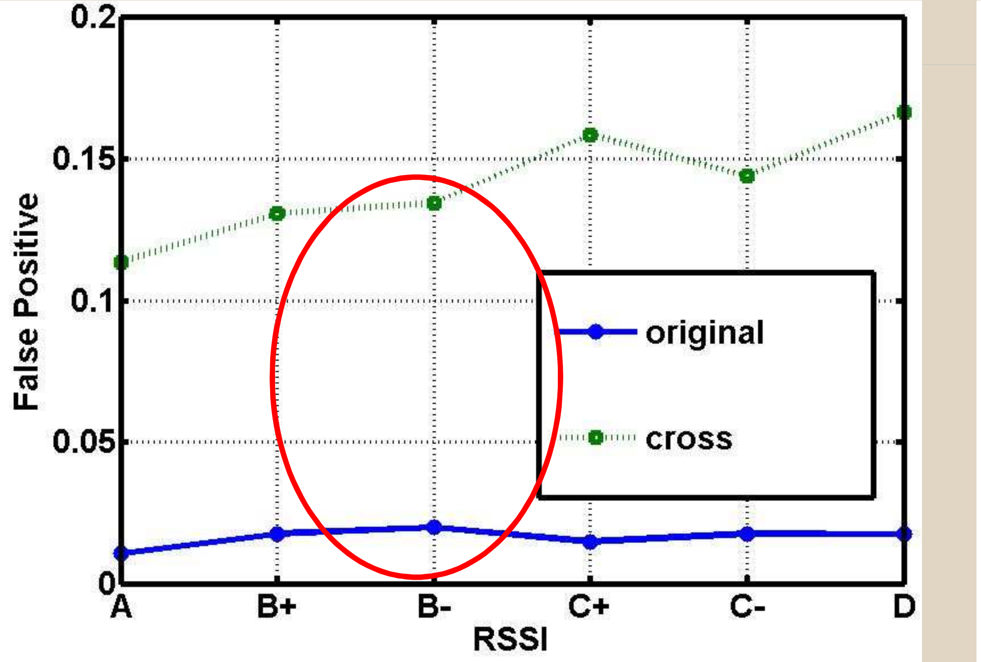
RSSI Range	A	B+	B-	C+	C-	D
802.11g(multi-TMM)	0%	0.77%	0%	0%	0%	0%
802.11b(multi-TMM)	0%	0.03%	0.02%	0.11%	0.73%	0.1%
802.11g(multi-HDT)	0%	0.96%	0.16%	0.13%	0.55%	0.96%
802.11b(multi-HDT)	0%	1.07%	1.16%	1.02%	1.36%	1.41%

Evaluation: *Cross-validation-- under different RSSI for TMM*

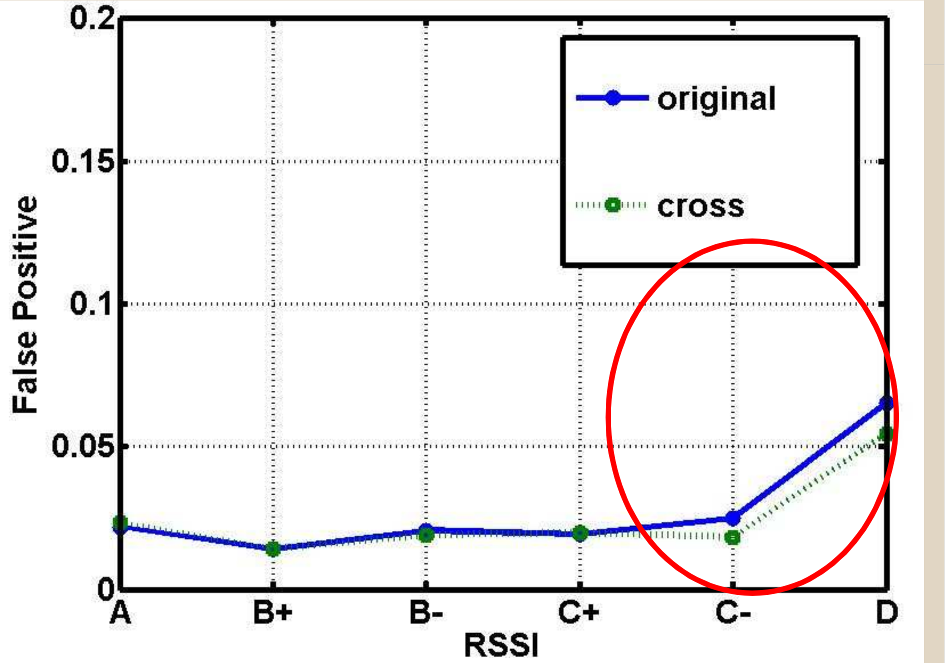


Evaluation: *Cross-validation-- under different locations*

TMM



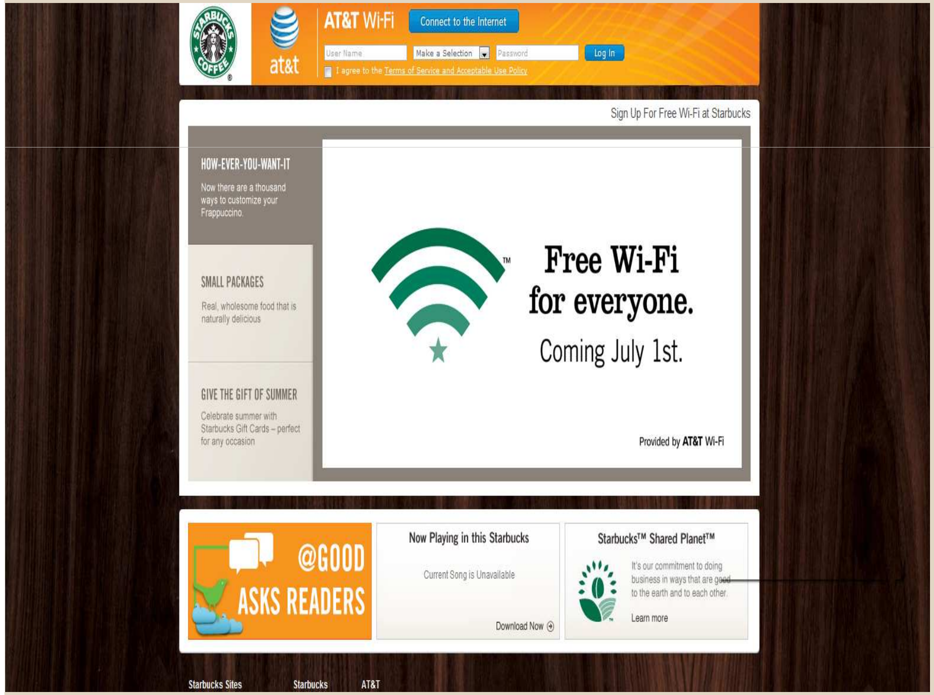
HDT



Homepage of AP

Starbucks

O'Hare International Airport



AT&T Wi-Fi

Connect to the Internet

User Name | Make a Selection | Password | Log In

□ I agree to the Terms of Service and Acceptable Use Policy

Sign Up For Free Wi-Fi at Starbucks

HOW-EVER-YOU-WANT-IT

Now there are a thousand ways to customize your Frappuccino.

SMALL PACKAGES

Real, wholesome food that is naturally delicious

GIVE THE GIFT OF SUMMER

Celebrate summer with Starbucks Gift Cards – perfect for any occasion

Free Wi-Fi for everyone.

Coming July 1st.

Provided by AT&T Wi-Fi

@GOOD ASKS READERS

Now Playing in this Starbucks

Current Song is Unavailable

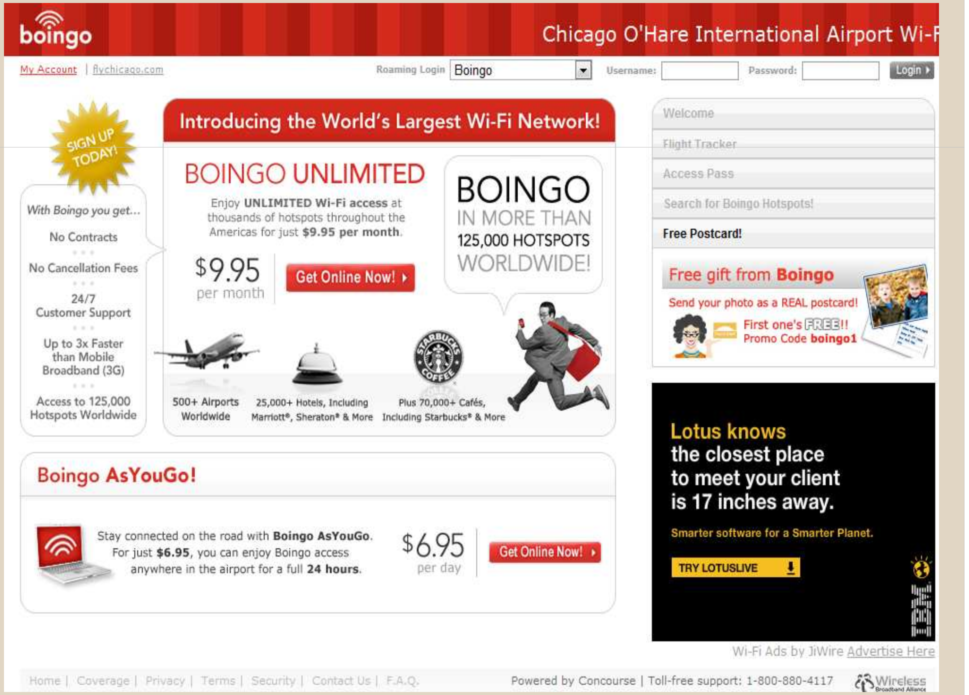
Download Now

Starbucks™ Shared Planet™

It's our commitment to doing business in ways that are good to the earth and to each other.

Learn more

Starbucks Sites | Starbucks | AT&T



boingo

Chicago O'Hare International Airport Wi-F

My Account | flychicago.com

Roaming Login: Boingo | Username: | Password: | Login

SIGN UP TODAY!

With Boingo you get...

No Contracts

No Cancellation Fees

24/7 Customer Support

Up to 3x Faster than Mobile Broadband (3G)

Access to 125,000 Hotspots Worldwide

Introducing the World's Largest Wi-Fi Network!

BOINGO UNLIMITED

Enjoy **UNLIMITED Wi-Fi access** at thousands of hotspots throughout the Americas for just **$9.95 per month**.

$9.95 per month

Get Online Now!

BOINGO IN MORE THAN 125,000 HOTSPOTS WORLDWIDE!

500+ Airports Worldwide

25,000+ Hotels, Including Marriott®, Sheraton® & More

Plus 70,000+ Cafés, Including Starbucks® & More

Welcome

Flight Tracker

Access Pass

Search for Boingo Hotspots!

Free Postcard!

Free gift from Boingo

Send your photo as a REAL postcard!

First one's FREE!!

Promo Code **boingo1**

Boingo AsYouGo!

Stay connected on the road with **Boingo AsYouGo**. For just **$6.95**, you can enjoy Boingo access anywhere in the airport for a full **24 hours**.

$6.95 per day

Get Online Now!

Lotus knows the closest place to meet your client is 17 inches away.

Smarter software for a Smarter Planet.

TRY LOTUSLIVE

IBM

Wi-Fi Ads by JiWire Advertise Here

Home | Coverage | Privacy | Terms | Security | Contact Us | F.A.Q.

Powered by Concourse | Toll-free support: 1-800-880-4117

Wireless Broadband Alliance