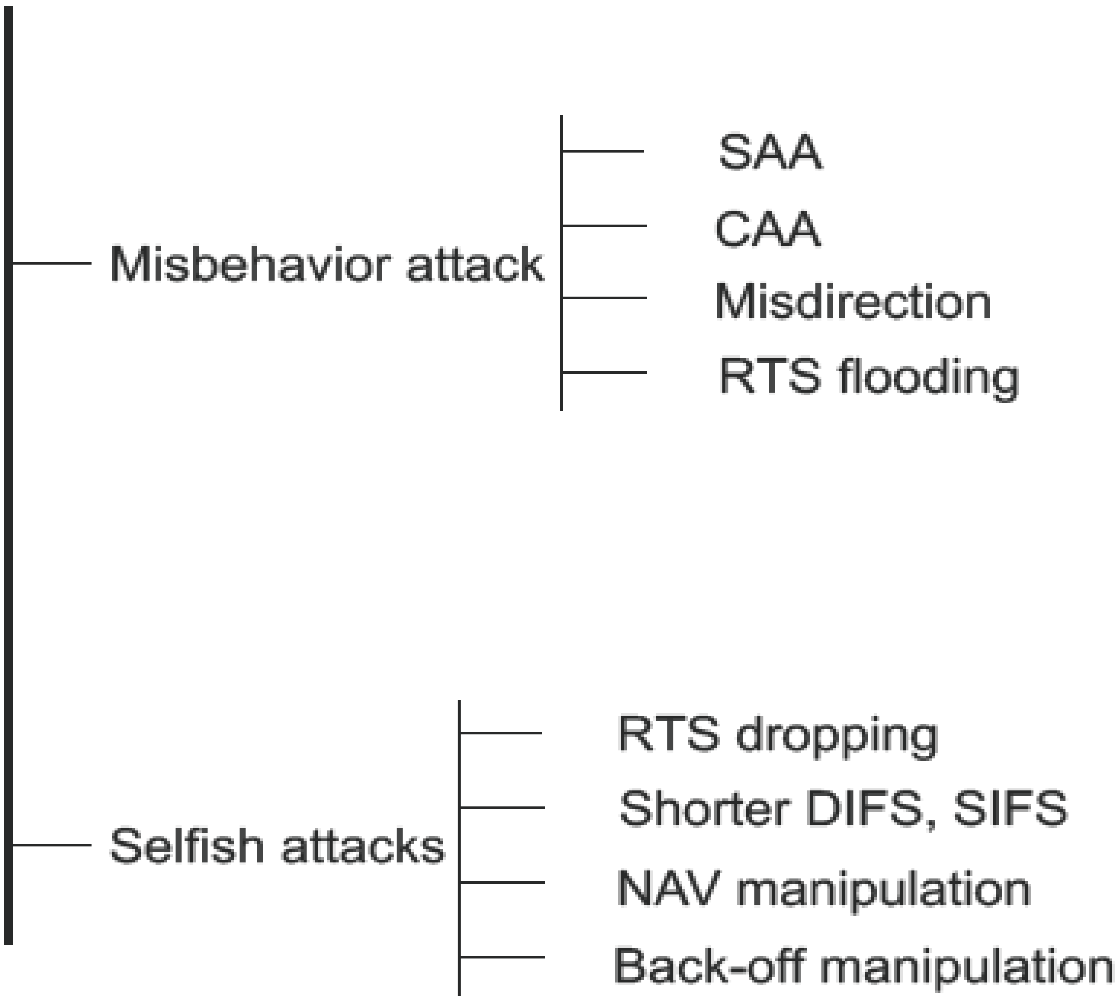
Real Time Detection of MAC Layer DoS Attacks in IEEE 802.11 Wireless Networks

Mallesham Dasari
Department of Computer Science
Stony Brook University
Email: mdasari@cs.stonybrook.edu

WINGS Lab

L2 DoS Attacks



MAC DoS Attacks

- Misbehavior attack
  - SAA
  - CAA
  - Misdirection
  - RTS flooding
- Selfish attacks
  - RTS dropping
  - Shorter DIFS, SIFS
  - NAV manipulation
  - Back-off manipulation

WINGS Lab

Change Point Detection

- Collect time series data
  - $\{x_1, x_2, x_3, \ldots\ldots\ldots, x_t, \ldots\ldots\ldots\}$
- Detect change point (μ), where the time series follows different distributions before and after the change
- Pre and post change density functions are
  - $f(.)$ and $g(.)$ respectively
- Hypotheses
  - $\mathcal{H}_0 = \{x_1, x_2, x_3, \ldots\ldots\ldots, x_n\} \sim f$
  - $\mathcal{H}_1 = \{x_1, x_2, x_3, \ldots\ldots\ldots, x_\mu\} \sim f$

    $\{x_{\mu+1}, x_{\mu+2}, x_{\mu+3}, \ldots\ldots\ldots, x_n\} \sim g$

WINGS Lab

Change Point Detection

- CUSUM family algorithms
  - Parametric
    - Cumulative sum of log likelihood ratio
      - $W_n = \{W_{n-1} + \log(g/f)\}^+$, for all n>0, $x^+ = \max(0, x)$
      - Use preset threshold for decision
  - Non parametric
    - Removed the need for density functions
      - $W_n = \{W_{n-1} + x_n - c\}^+$, for all n>0
      - x_n is a non parametric score, a special heuristic function

- Similarly, R-SPRT

Central Limit Theorem

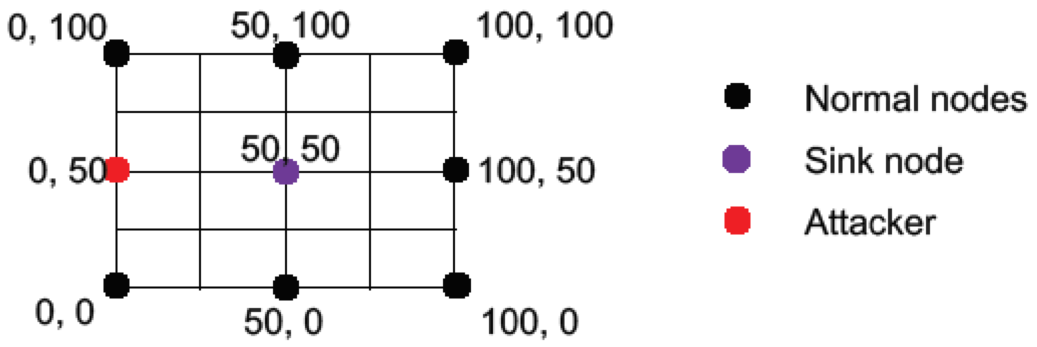
- New sequential change point detection
  - Let *m* is the window size, $0 \leq t \leq n-2m$
  - $Y_1(t) = \sum_{i=t+1}^{t+m} xi$ and $Y_2(t) = \sum_{i=t+m+1}^{t+2m} xi$
  - $D(t) = | Y_1(t) – Y_2(t) |$
- Compare $D(t)$ with threshold (D_{th})
- What makes it so Special?
- Let ϕ(.) be the CDF for standard normal distribution, defined as below:
  - ϕ(z) = P(a ≤ z)

Computing Threshold

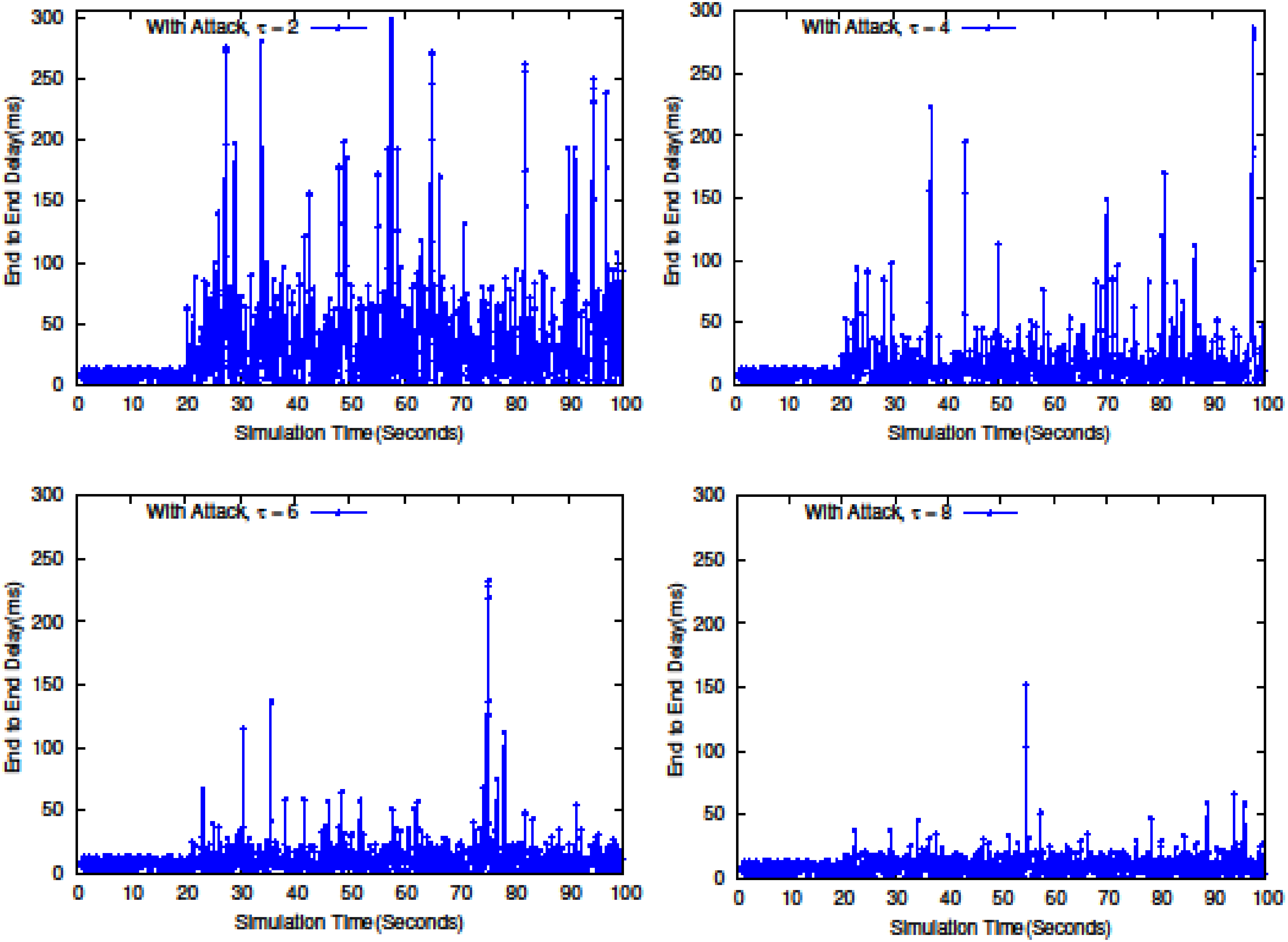
- Then, $1 - \phi(z)$ is the probability of $P(a > z)$
- For desired false alarm rate (ε), the cut-off value of z can be calculated as:
  - $1 - \phi(z) = \varepsilon$
- Borrow the solution z from the above, and scale it to find the threshold as below:
  - $D_{th} = z\sqrt{2m}\sigma$
- Detection Latency:
  - Report change time: ɥ = t+m
  - Latency: ɥ - μ

Attack Simulation

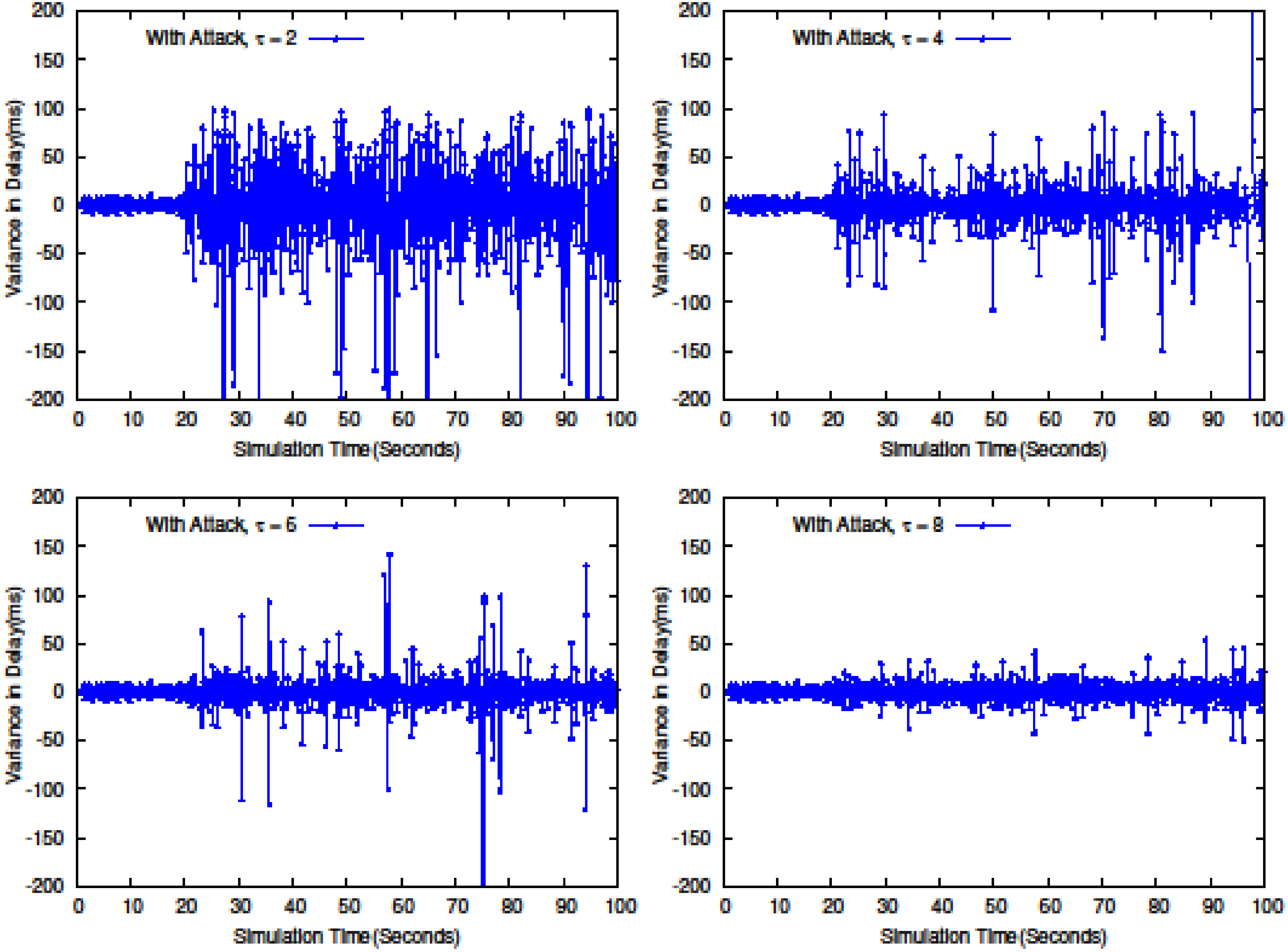
- Back-off manipulation attacks
  - DIFS, SIFS, slot time
- RTS flooding attack
- UDP echo client application
- Different inter packet departure rates

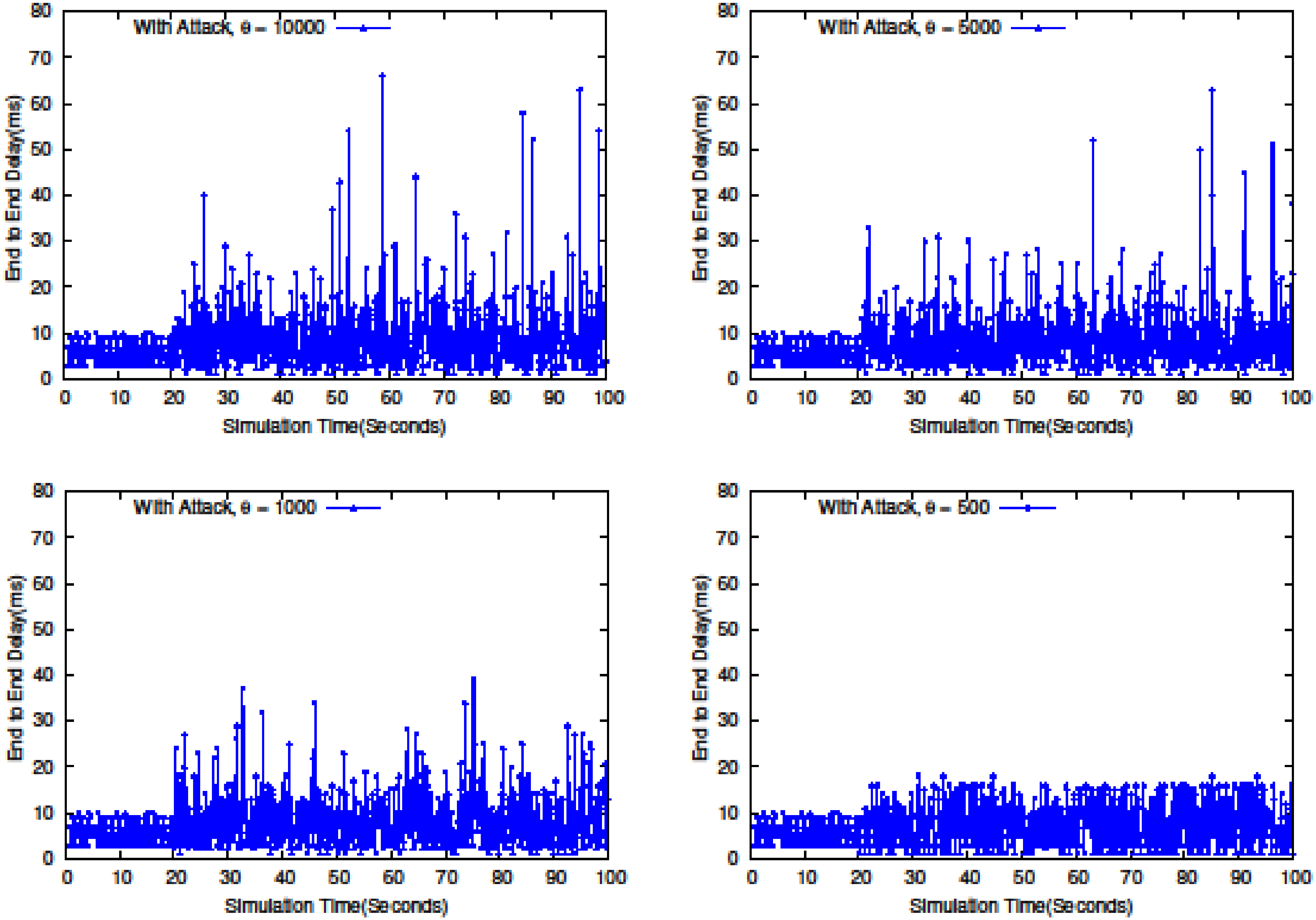


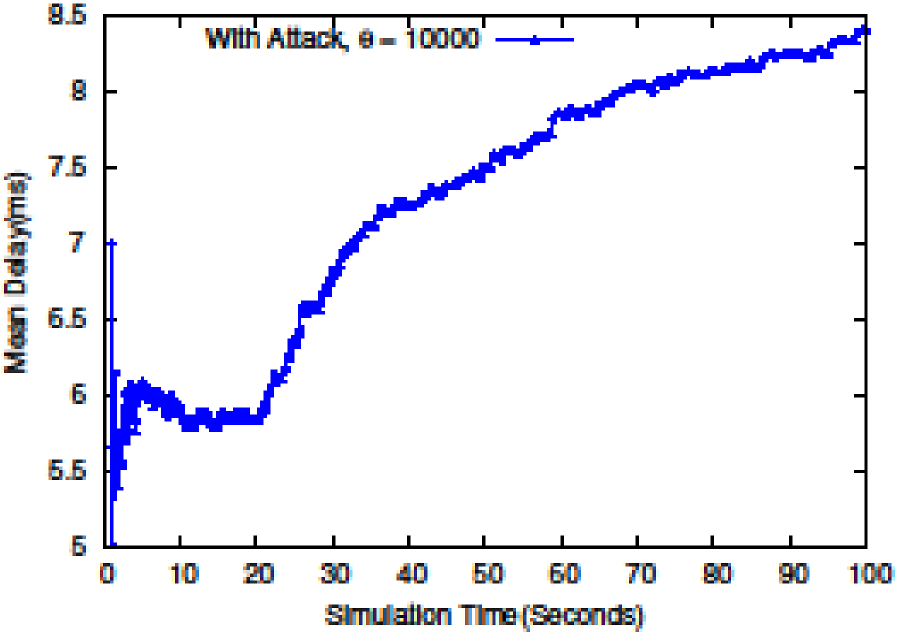
WINGS Lab

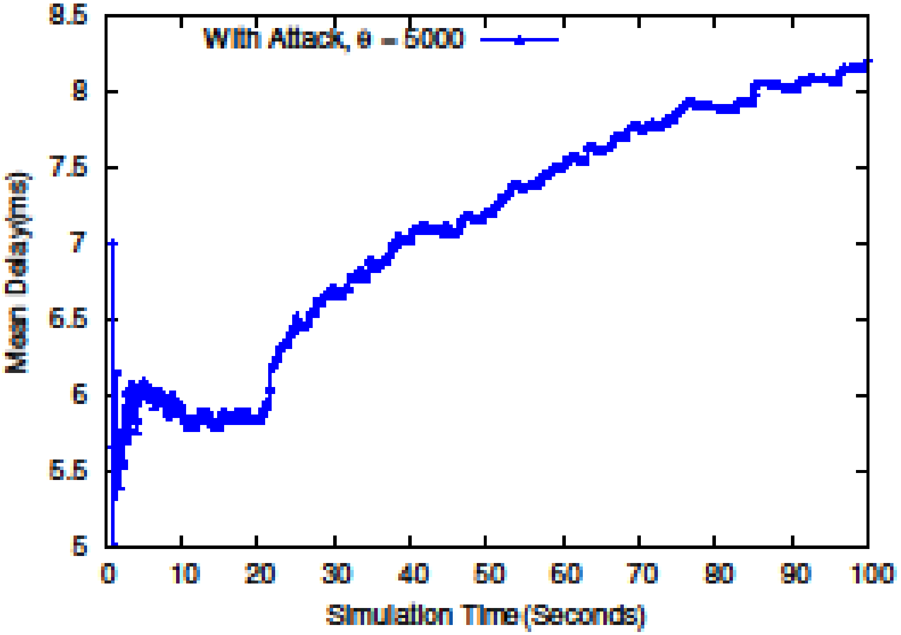


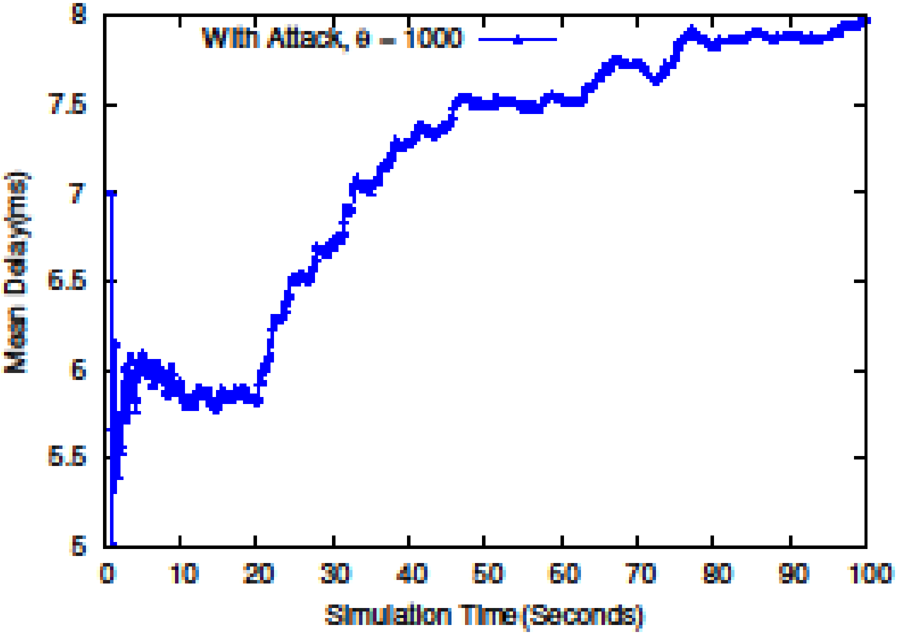
With Attack, τ = 2
With Attack, τ = 4
With Attack, τ = 6
With Attack, τ = 8
End to End Delay(ms)
Simulation Time (Seconds)
0
50
100
150
200
250
300
0
10
20
30
40
50
60
70
80
90
100

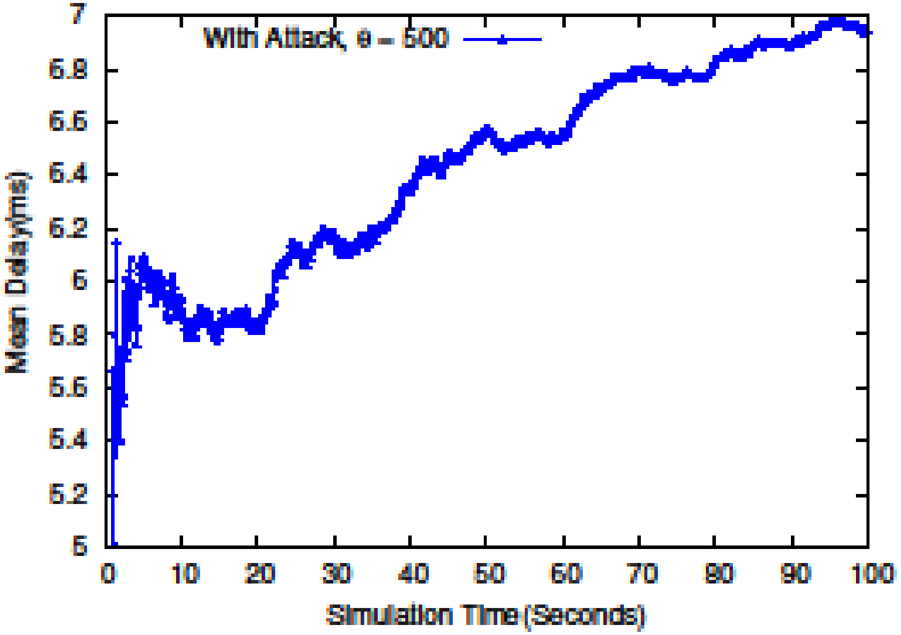

With Attack, τ = 2
With Attack, τ = 4
With Attack, τ = 6
With Attack, τ = 8
Variance in Delay(ms)
Simulation Time (Seconds)
200
150
100
50
0
-50
-100
-150
-200
0
10
20
30
40
50
60
70
80
90
100


With Attack, θ = 10000
With Attack, θ = 5000
With Attack, θ = 1000
With Attack, θ = 500
End to End Delay(ms)
Simulation Time(Seconds)
0
10
20
30
40
50
60
70
80
90
100

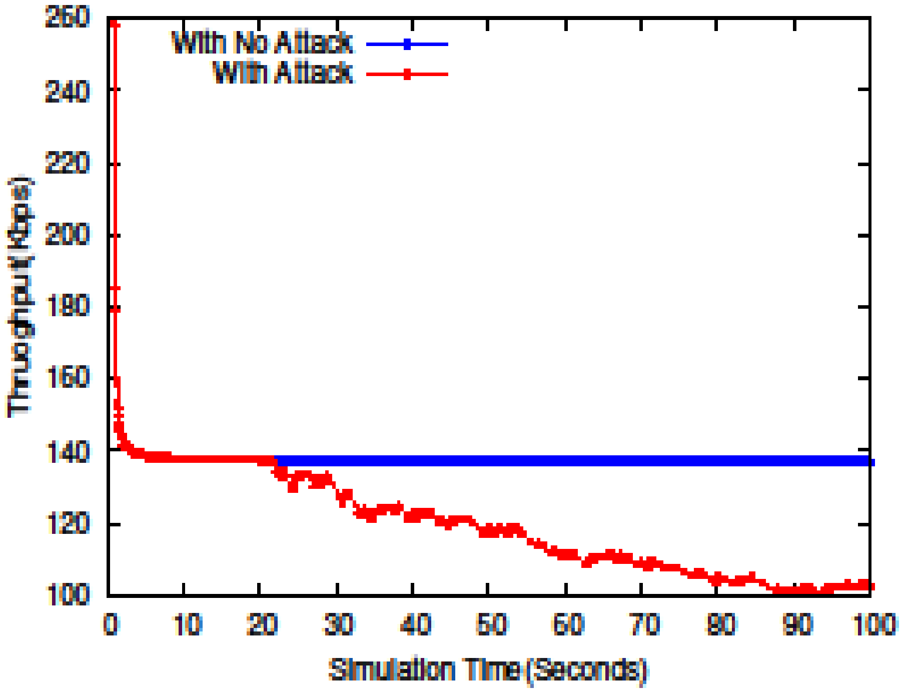

With Attack, θ = 10000
Mean Delay(ms)
8.5
8
7.5
7
6.5
6
5.5
5
0
10
20
30
40
50
60
70
80
90
100
Simulation Time (Seconds)

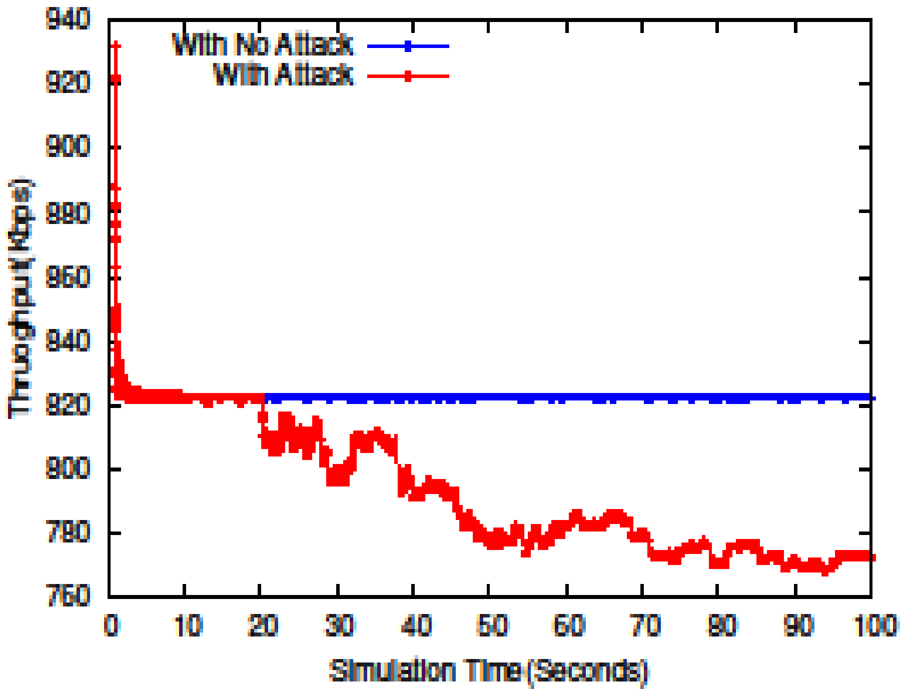

With Attack, θ = 5000
Mean Delay(ms)
8.5
8
7.5
7
6.5
6
5.5
5
0
10
20
30
40
50
60
70
80
90
100
Simulation Time (Seconds)


With Attack, θ = 1000
Mean Delay(ms)
8
7.5
7
6.5
6
5.5
5
0
10
20
30
40
50
60
70
80
90
100
Simulation Time (Seconds)


With Attack, θ = 500
Mean Delay(ms)
7
6.8
6.6
6.4
6.2
6
5.8
5.6
5.4
5.2
5
0
10
20
30
40
50
60
70
80
90
100
Simulation Time (Seconds)

Throughput Curves





WINGS Lab

Detection Accuracy

Algorithms	Scenarios	Detected	False Alarms	Latency(s)
CLT*	1	Yes	2	2.988
CLT*	1	Yes	8	7.223
CLT*	2	Yes	0	0.029
CLT*	2	Yes	1	0.818
NP-CUSUM	1	Yes	>50	-
NP-CUSUM	2	No	-	-

The higher latencies are corresponding to higher E-to-E delays

Why so?

WINGS Lab

Takeaways

- Time series based attack detection
- A new sequential change point detection based on CLT
- Non parametric, Dynamic threshold
- Two types of 802.11 attacks
- NS-3 802.11 stack hack to create attackers

THANKS!

Questions

Email: mdasari@cs.stonybrook.edu
WINGS Lab
Department of Computer Science
Stony Brook University