Towards Modeling Wireless Location Privacy

Leping Huang, Hiroshi Yamane, Kanta Matsuura, Kaoru Sezaki

NOKIA

Motivation

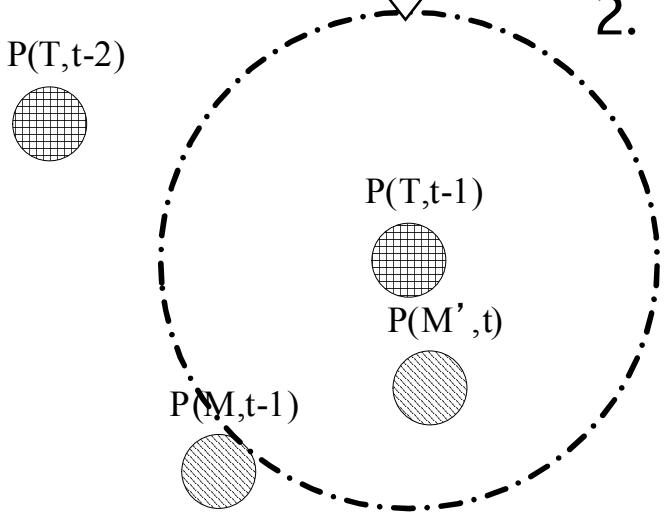
Location Tracking/Privacy Problem

Correlation Attack

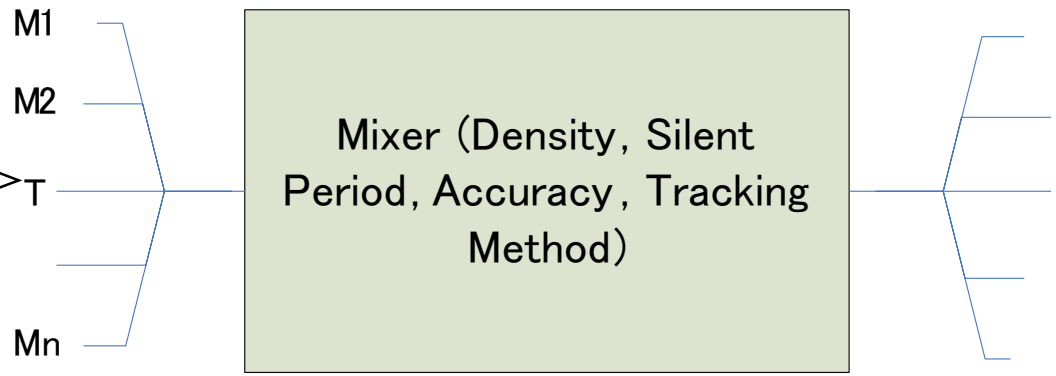
Anonymous Communication /PET

Mix

1. Evaluation of protocol
2. Reuse of research result



Modeling



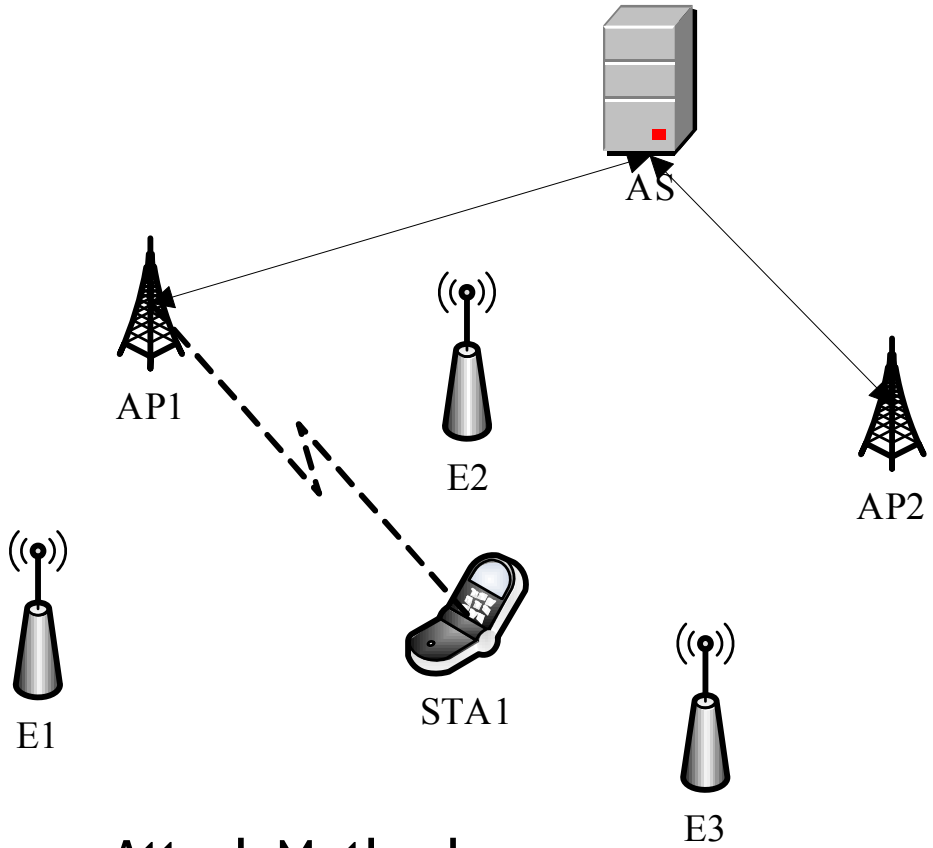
NOKIA

Outline

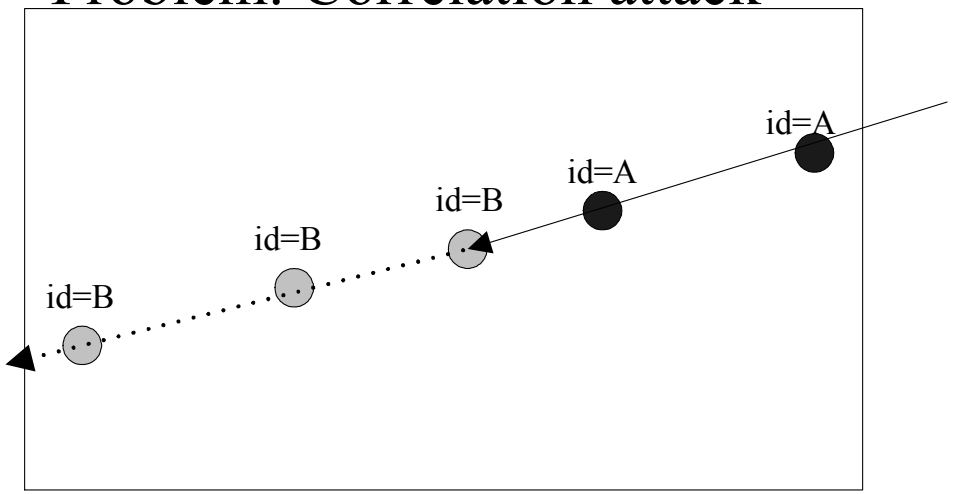
- Background
  - Location privacy problem
  - Correlation Attack and Silent Period
- Formal model
- Simulation study: Silent period
- Extension and Discussion
- Conclusion

NOKIA

Informal Description of Wireless Location Privacy



Problem: Correlation attack

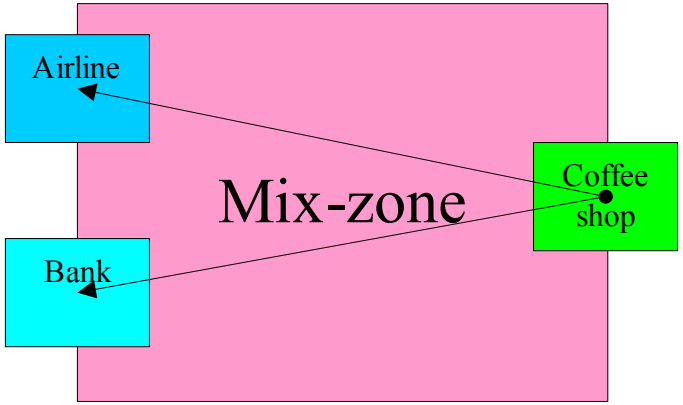


Attack Method:

1. RSSI/TOA based on triangulation
2. Use correlation between old and new MAC

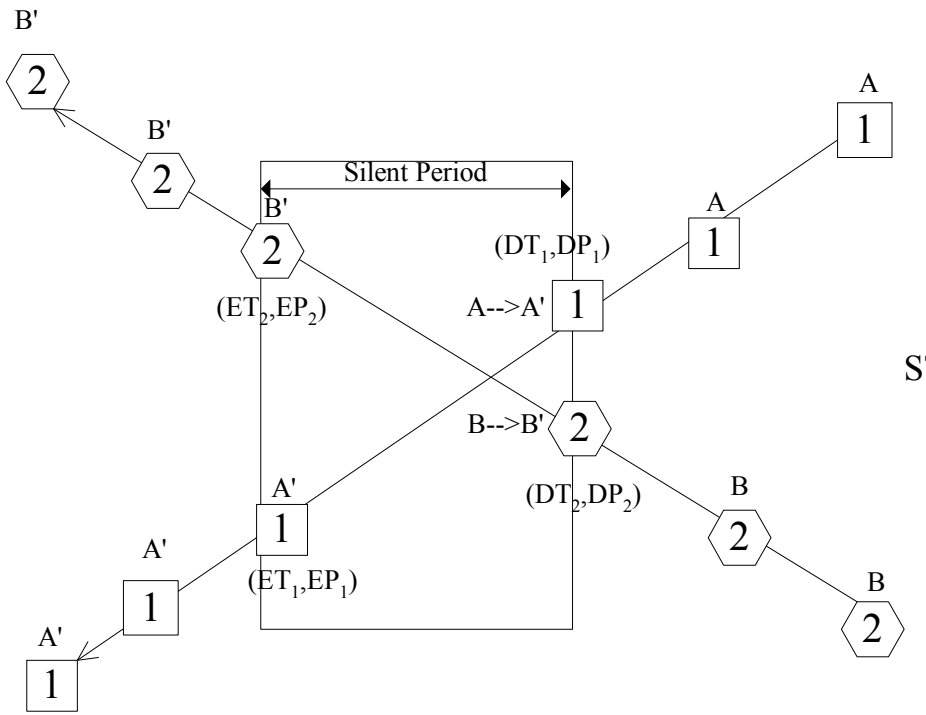
Prior Arts

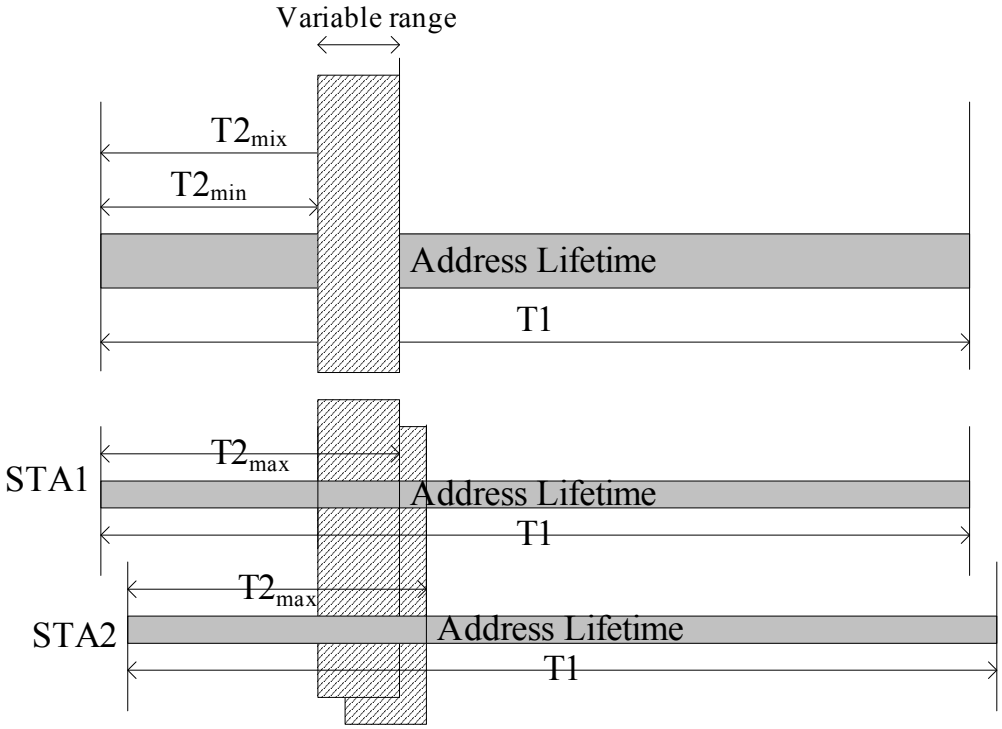
- Mix-Zone(Beresford, Stajano)



- Bluetooth 1.2, WLAN
  - Disposable MAC address
  - Update after every association (about once 30 minutes)
  - Can not prevent correlation attack

Our Previous Proposal: Silent Period

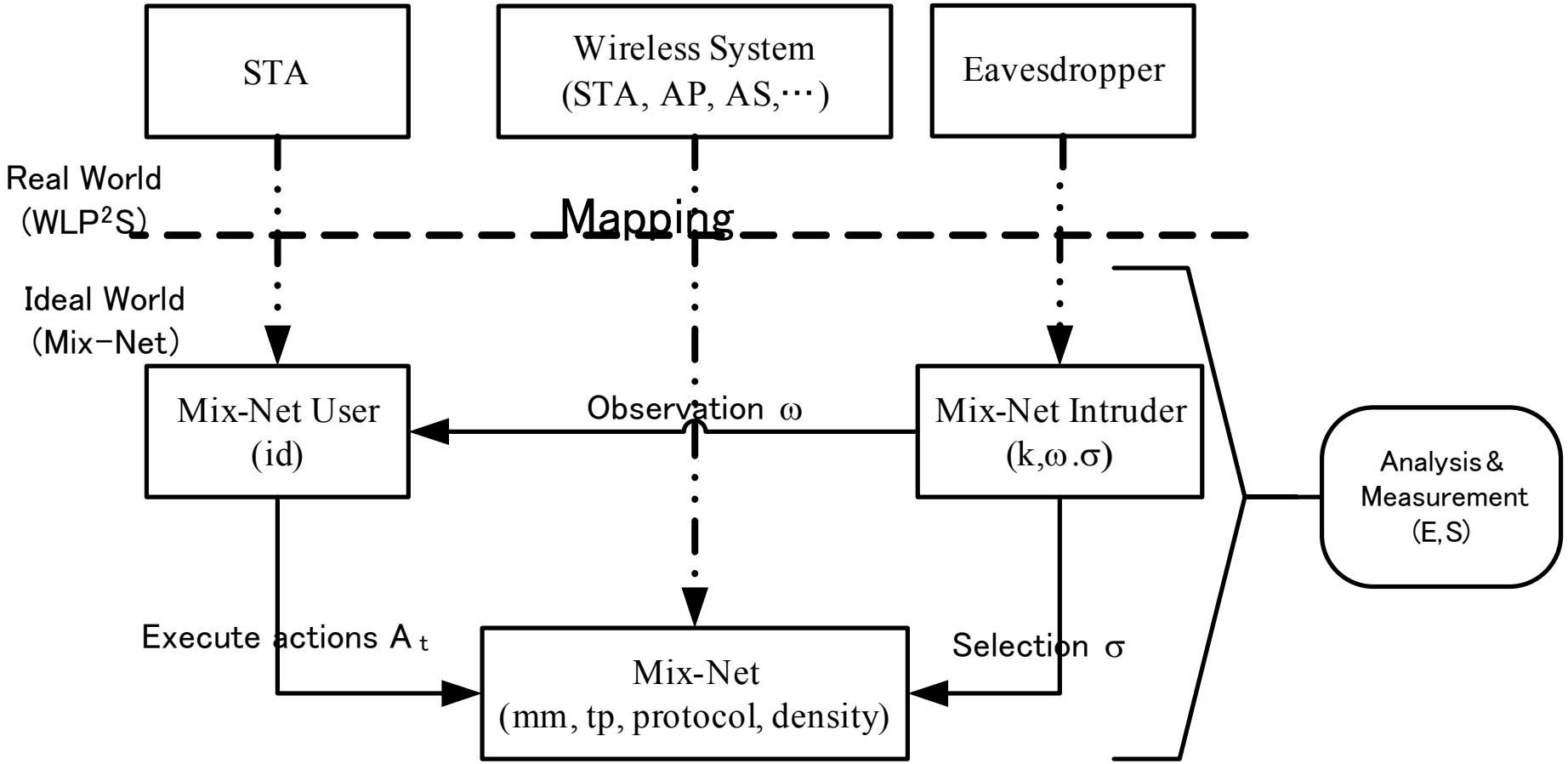




T1: Address change period
T2: Lifetime

- Variable Part: mix temporal relation
- Constant Part: mix spatial relation

Formal Model

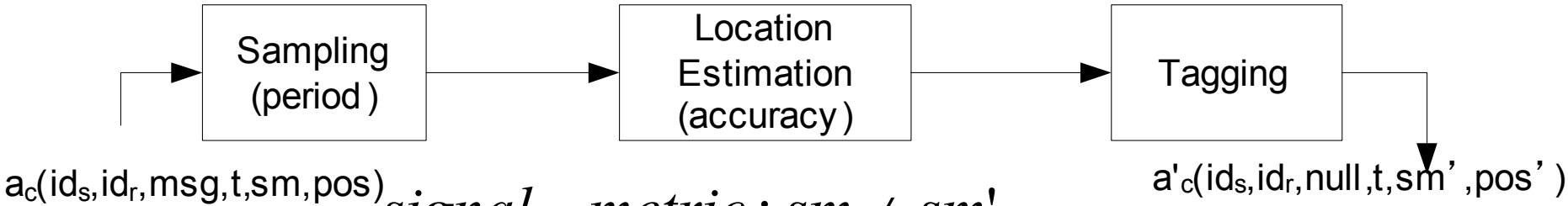


Observation Function

2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration / ID	A1	A2	A3	Sequence Control	A4	Frame Body	FCS

$$a(id_s, id_r, msg, sm, pos)$$

- Observation function



$$signal\_metric: sm \neq sm'$$

$$position: \quad pos \neq pos'$$

Feature: observation functions bring bias and loss on actions

Analogous to positioning algorithm

Selection function and anonymity definition

- Analogous to tracking algorithm
- Trail: a set of actions with same id
  - Input: trails (id, time, position)
  - output: probability of linkability
- Equivalence relation

$$\sim_{w(Tr)}$$

- Probability of Linkability

$$p_{i,j} = P\left(Tr_i \sim_{w(T_r)} Tr_j\right)$$

NOKIA

Anonymity and Its Measures

Geographical Anonymity Set(GAS)

$$GAS(id_i) = \{id_j \mid id_j \in ID, \exists Tr_i, Tr_j \in Tr, p(i,j) \neq 0\}$$

Measures:

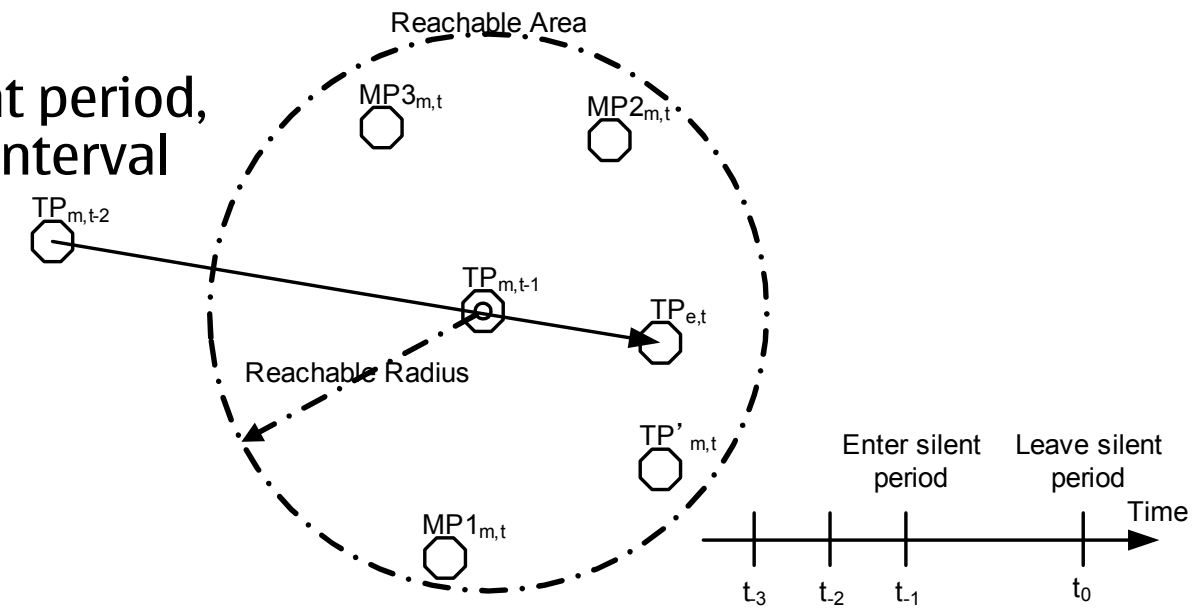
$$Size : S = |GAS(id_i)|$$

$$Entorpy : E = \sum p_{i.j} \log_2 p_{i.j}$$

NOKIA

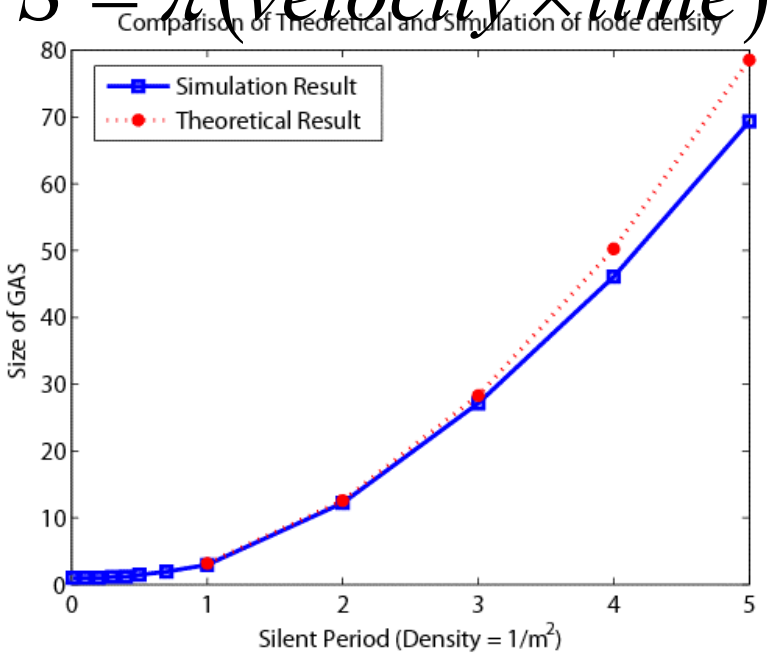
Evaluation of Silent Period Protocol

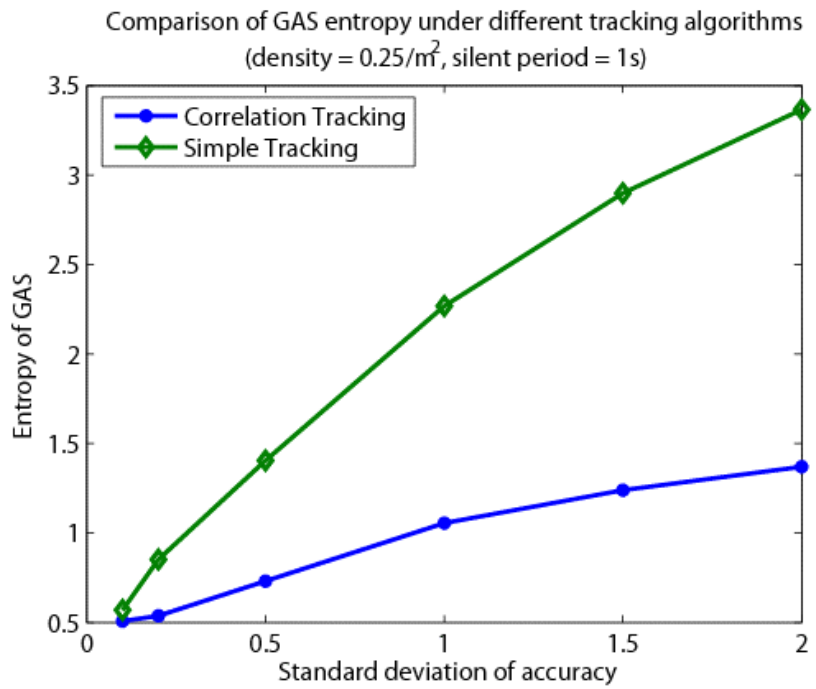
- Tracking algorithm (selection function)
  - Simple tracking
  - Correlation Tracking
- Positioning algorithm (observation function)
  - Sampling interval, uniform error
- Random Walk over 20m*20m
- Evaluated Parameters:
  - node density, length of silent period, lifetime, accuracy, sampling interval
- Measures
  - Size and entropy of GAS



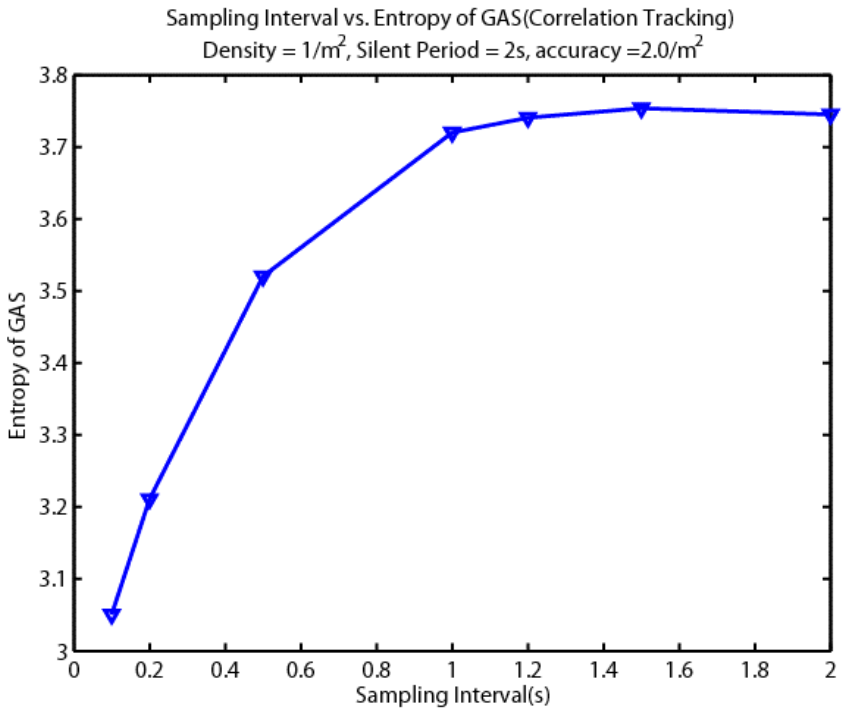
Result 1

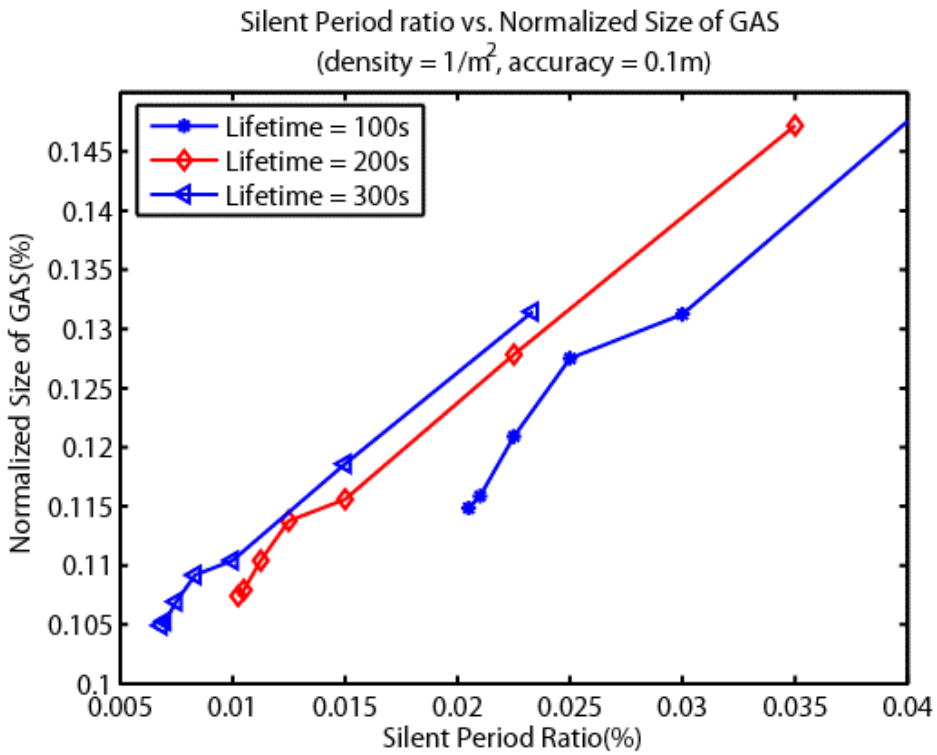
$$S = \pi(velocity \times time)^2 \times density$$





Result 2


Sampling Interval vs. Entropy of GAS(Correlation Tracking)
Density = 1/m2, Silent Period = 2s, accuracy =2.0/m2
Entropy of GAS
Sampling Interval(s)
3.8
3.7
3.6
3.5
3.4
3.3
3.2
3.1
3
0
0.2
0.4
0.6
0.8
1
1.2
1.4
1.6
1.8
2

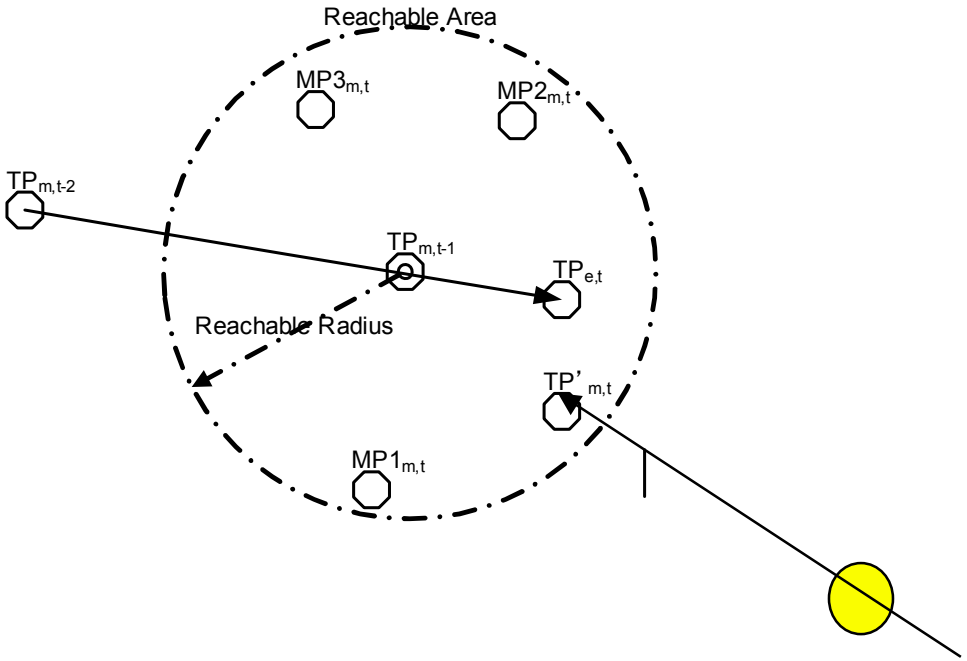

Silent Period ratio vs. Normalized Size of GAS
(density = 1/m2, accuracy = 0.1m)
Lifetime = 100s
Lifetime = 200s
Lifetime = 300s
Normalized Size of GAS(%)
Silent Period Ratio(%)
0.145
0.14
0.135
0.13
0.125
0.12
0.115
0.11
0.105
0.1
0.005
0.01
0.015
0.02
0.025
0.03
0.035
0.04

Role of system's parameters

Parameters	Affected Privacy Measure	Effect
Density	Size	larger -> larger
Length of Silent period	Size	Larger -> larger
Length of Lifetime	Size	Longer -> smaller (unsync case only)
Length of silent ratio	size	Larger -> larger (normalized)
Tracking Accuracy	Entropy	Higher -> smaller
Tracking Algorithm	Entropy	Advanced → smaller
Sampling interval	Entropy	Larger -> larger

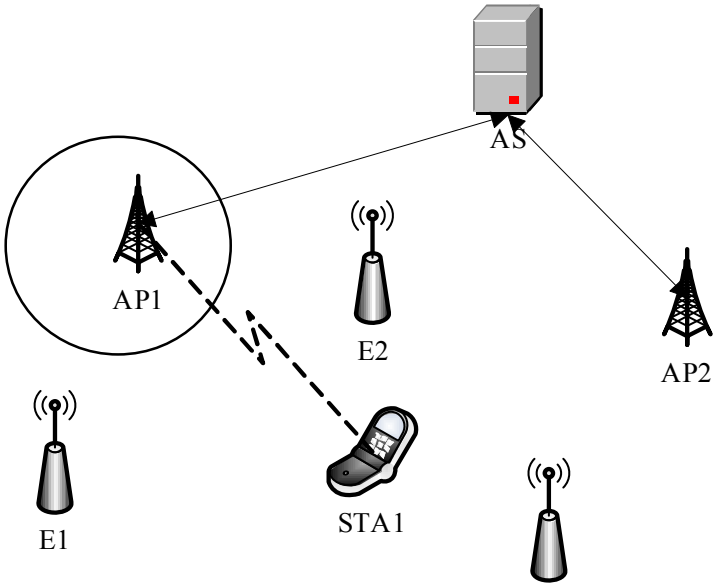
Protocol Extension based on Mix (1)

- Selective Attack/Intersection Attack
  - Advanced tracking algorithm

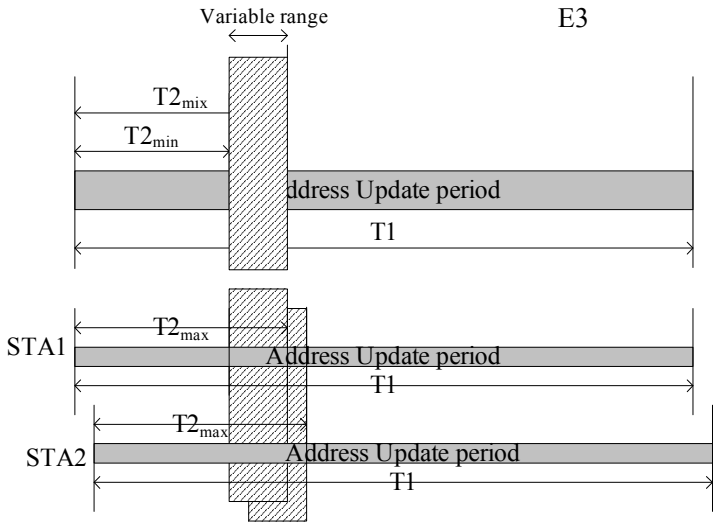


Protocol Extension based on Mix (2)

- Now: Gossip based system
- Controllable Mix-Net
  - *Decide the length of silent period based on registered node*



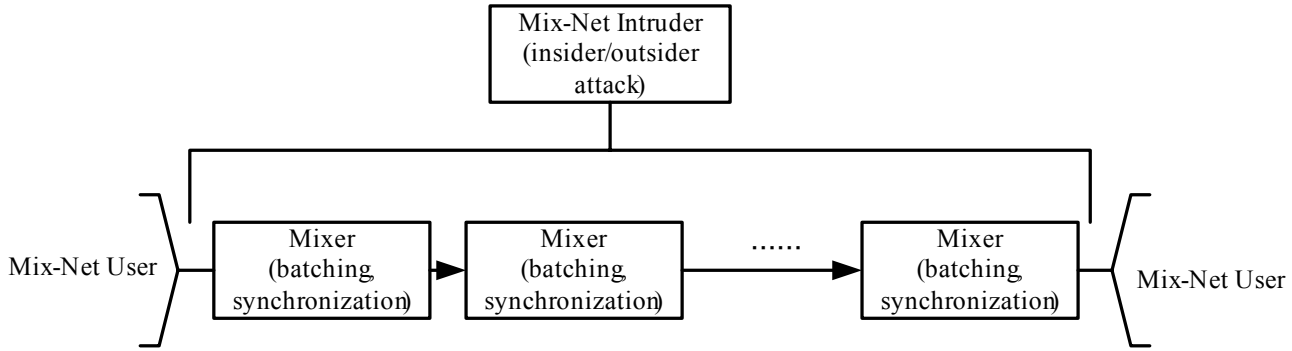
- Variable Silent Period
  - Mix batching algorithm
    - Timed mix
    - Timed pool mix etc



T1: Address change period
T2: Minimum silent period

Protocol Extension based on Mix (2)

- Mix-Cascade
  - Accumulated anonymity
  - Avoid single point of failure



Summary

- What we did not do
  - New type of mix: **NO,** standalone mix
  - New measures: **NO**, entropy/size
- What we did
  - Formal model as a bridge
  - Main point: Observation/selection function
- Application of formal model
  - Simulation on silent period
  - Extension of attack/defense model