Spatio-Temporal Access Control

Shu Chen
Advisor: Wade Trappe
WINLAB, Rutgers University

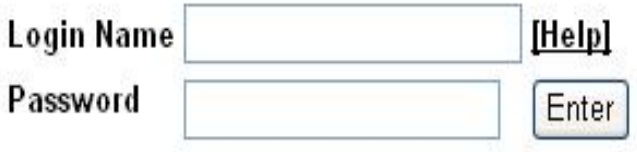
WIRELESS INFORMATION NETWORK LABORATORY

Outline

- Introduction of STAC
- STAC Model
- Seamless Feeding Architecture for STAC
- Summary

Introduction to STAC

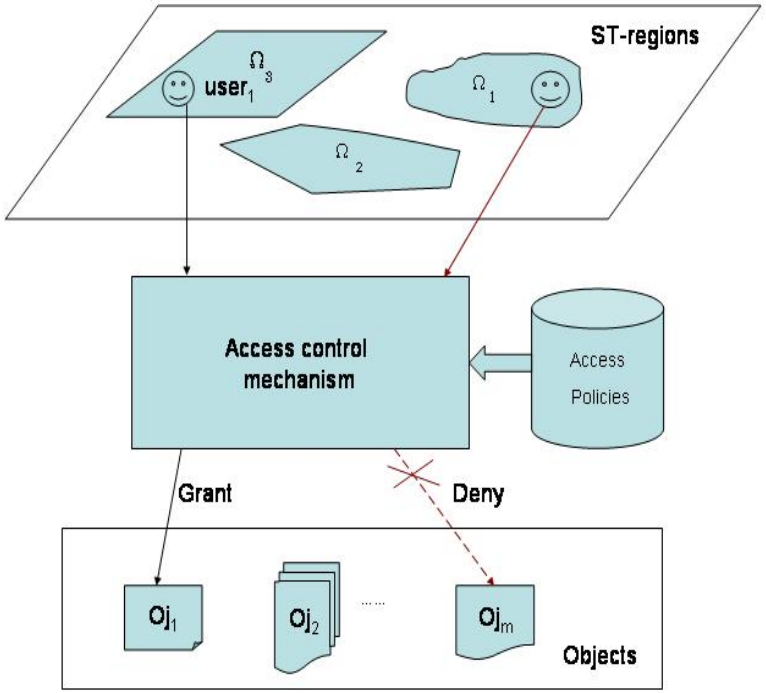
- What is the *conventional* way to authenticate the access to a resource?



Identity check

- Identity Based Access Control (IBAC) is inconvenient and unnecessary in certain types of scenarios.
- Instead, a user's *spatio-temporal* context is more desirable for basing access control upon.
  - E.g. A company may restrict its confidential documents so that they can only be accessed while inside a building during normal business hours.
- *Spatio-Temporal Access Control (STAC)* allows for objects to be accessed only if the accessing entity is in the right place at the right time.

STAC Model



- Five basic components
  - Users: USERS
  - Objects: OBS
  - Operations: OPS
  - Permissions:
    $PRMS \subseteq 2^{(OPS \times OBS)}$
  - Spatio-temporal regions: ST-regions
- Access policies

What makes STAC different from conventional AC systems?

The definition and representation of Objects, ST-regions and Access Policies.

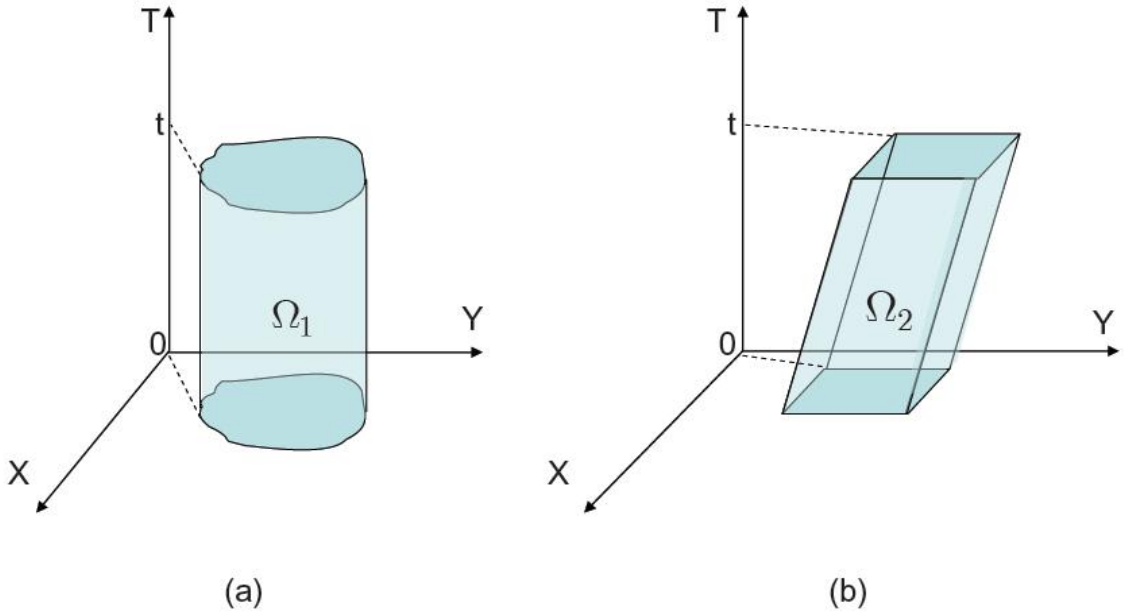
STAC Components-1

- Objects: endowed with temporal character
  - Static
  - Streaming: continually evolves with time
    - E.g. a movie *Mv* broadcast to the entire network
    - Break down streaming objects into pieces
      - *Mv = { Mv_1[0 , 10), Mv_2[10,20), Mv_3[20,30) }*
      - *Object atom: the smallest constituent piece that a larger object can be decomposed, decided by the temporal resolution of a STAC system.*

- ST-region: a set of 3-tuple Ω={(x, y, t): valid areas in space and time}
  - Visualize as a continuous region instead of a set of discrete points
  - A ST-region Ω is called the *secure ST-region of (ob, op)* if the operation *op* is allowed to be performed on the object *ob* at Ω.

STAC Components-2

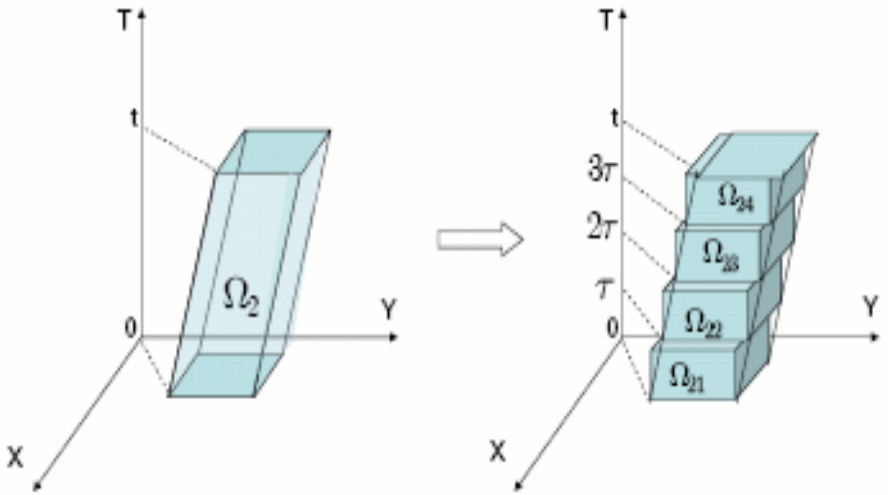
Examples of ST-regions



- Ω_1 : a spatial region that is constantly specified from time 0 to time *t*
- Ω_2 : a spatial region that varies with time. It requires that a user must move in a specific manner in order to maintain access privileges to an object.

STAC Components-3
Decomposing a ST-Region

- Granulate the ST-regions into atom ST-regions.
- Approximate each atom ST-region as a spatially constant region.
- Facilitate the enforcement of some policies by decomposing ST-regions and objects.



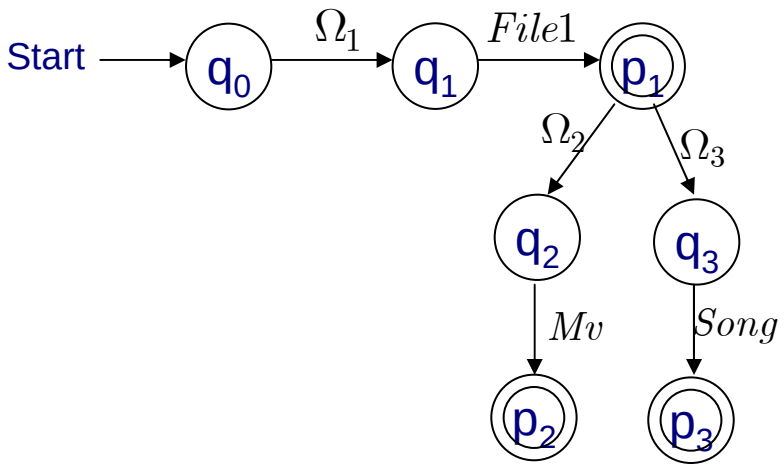
STAC Components-4

Access policies and their representations

- Basic policy: A = {(Ω;*op*;O_j)}, interpreted as within the ST-region Ω, the operation *op* on object O_j is approved.
  - Access Control Matrix is naturally used to represent basic policies.

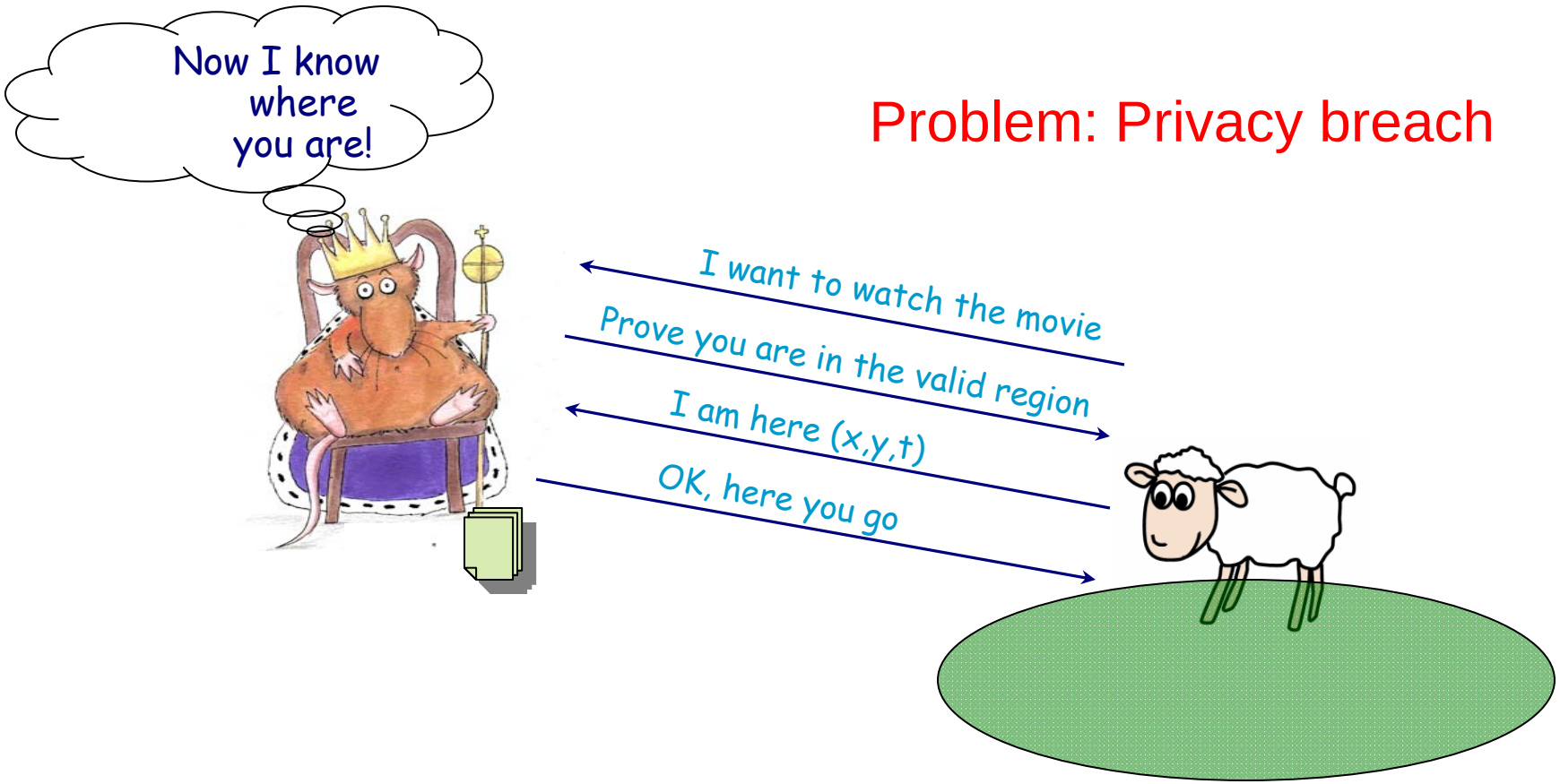
	Oj_1	Oj_2	……	Oj_m
Ω_1	1	rw_		101
Ω_2	0	r__		000
Ω_3	0	r_x		001

- Stateful policy: Historical information is needed. What you are allowed to access depends on what you've previously accessed.
  - Finite Automata is convenient for representing stateful policies.



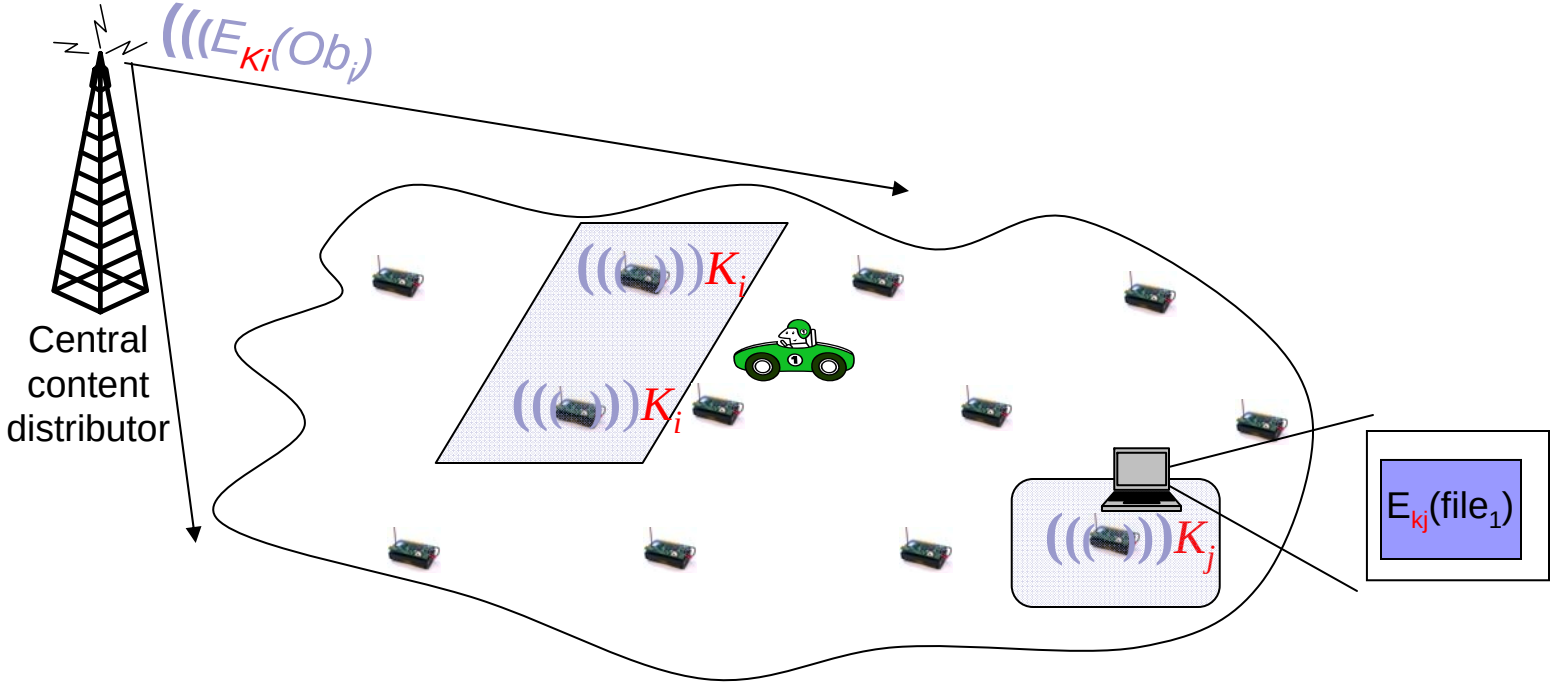
How to enforce STAC?

- Centralized Interacting Architectures



Problem: Privacy breach

STAC through Seamless Feeding Architecture



- Objects: Encrypted with keys and broadcasted to the entire network
- Wireless nodes: Inject decryption keys to their transmission scope as scheduled
- Mobile users: Have to appear at the right place at right time to get the decryption keys.

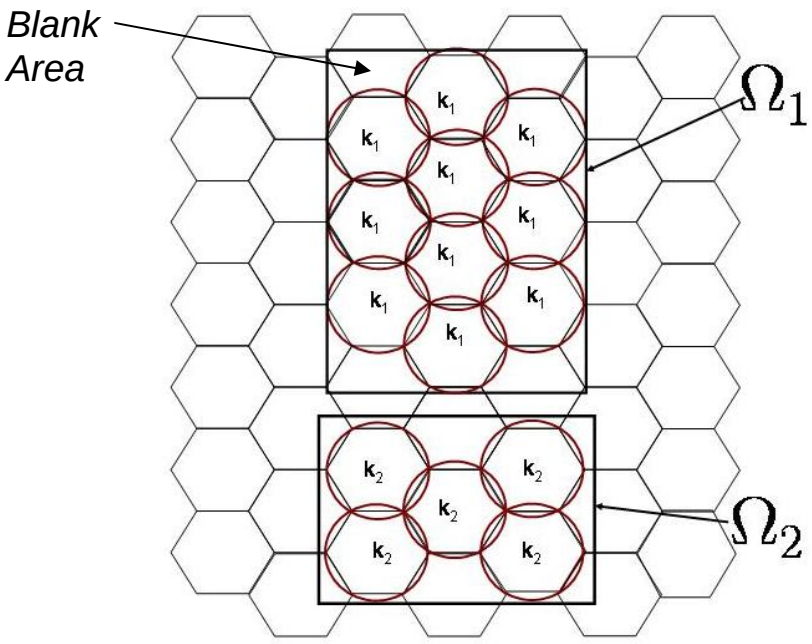
No localization is needed;

Users don't interact with any other entity!

Wireless Nodes Deployment & Key Assignment

- Basic scheme:
  - The region of interest is divided into regular hexagons.
  - One node is deployed at the center of each hexagon.
  - Each node's radio is isotropic and with radius *r=a*,
    a = the length of hexagon edge.

Caveat: In reality, propagation does not terminate suddenly!!!



E.g. :

Policy---

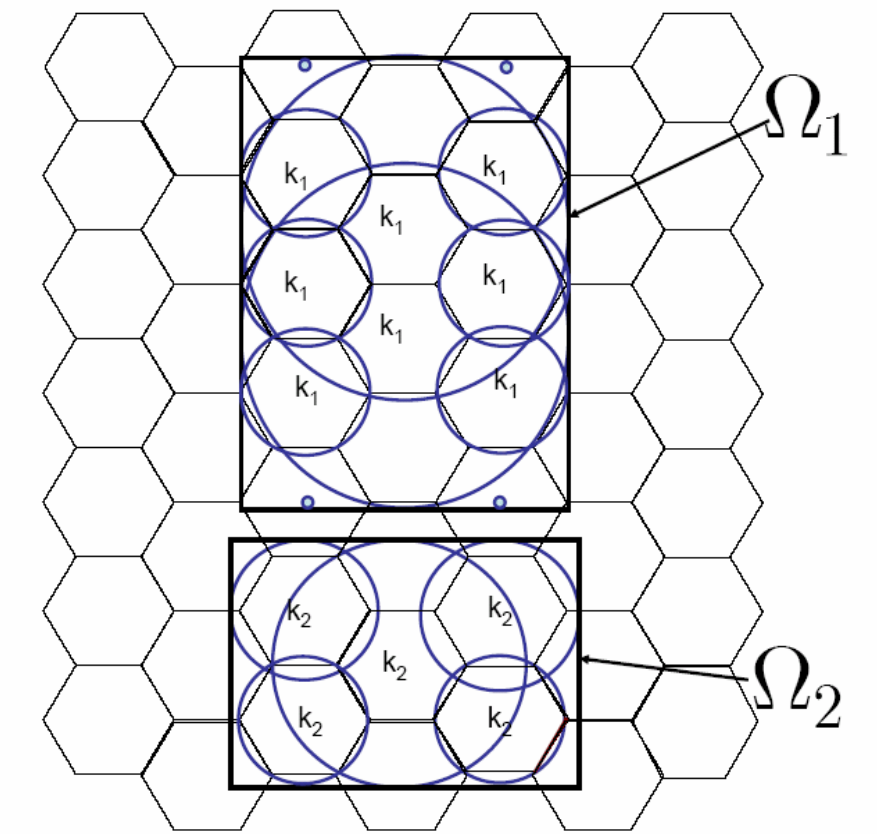
O_1 can be accessed only within Ω_1; O_2 can be accessed only within Ω_2

Scheme---

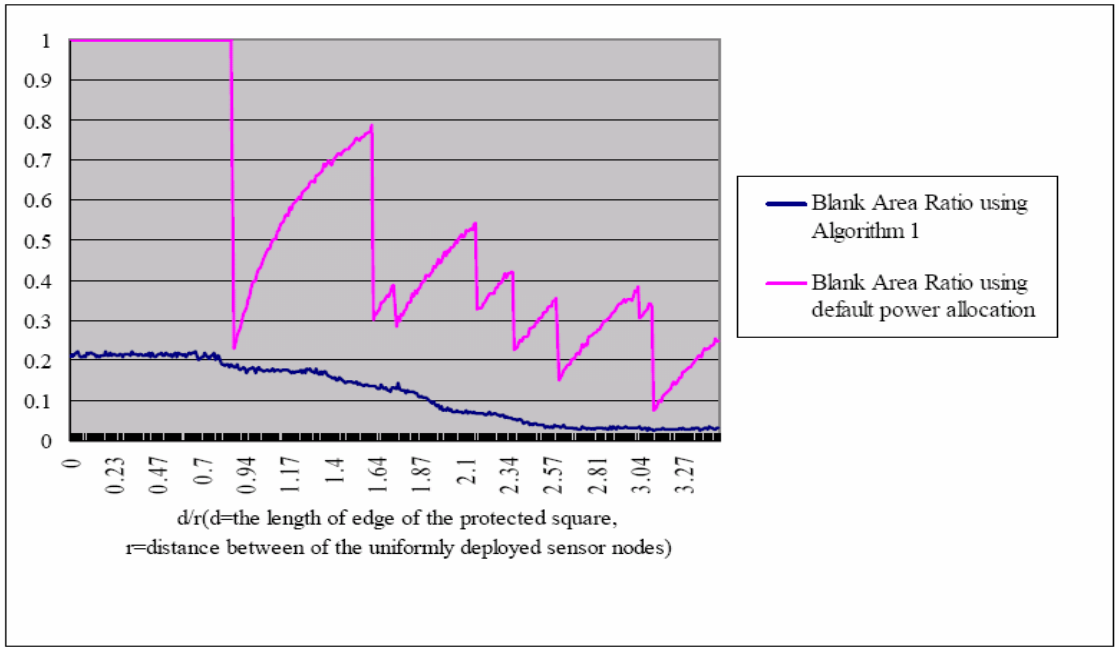
- Encrypt O_1 and O_2. $k_1$and k_2 are their decryption keys respectively.
- Assign k_1 to all the nodes whose radio discs are inside the rectangle $\Omega_1$and k_2 to the nodes whose radio discs are inside Ω_2

Improving the Coverage by Power Allocation Adjustment

- Security point of view:
  - Keys leak outside the desired ST-region is considered as security weakness.
- Aims at best cover from inside the region
- Algorithm:
  - For each node, allocate the power that maximally cover the region from inside, according to some propagation model.
  - Remove the redundant nodes or power assignment



Simulation Result



- *Blank area ratio=* $\dfrac{\text{Uncovered area}}{\text{Desired ST-region area}}$

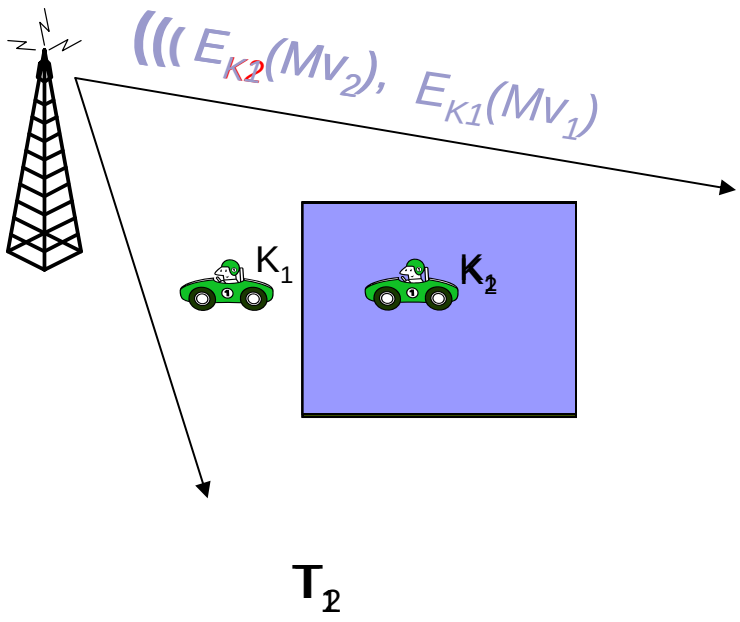
- In the simulation:
  - The desired ST-region is a square spatial region with sides of length *d*.
  - Change the density of the sensor nodes, distance between nodes *r*

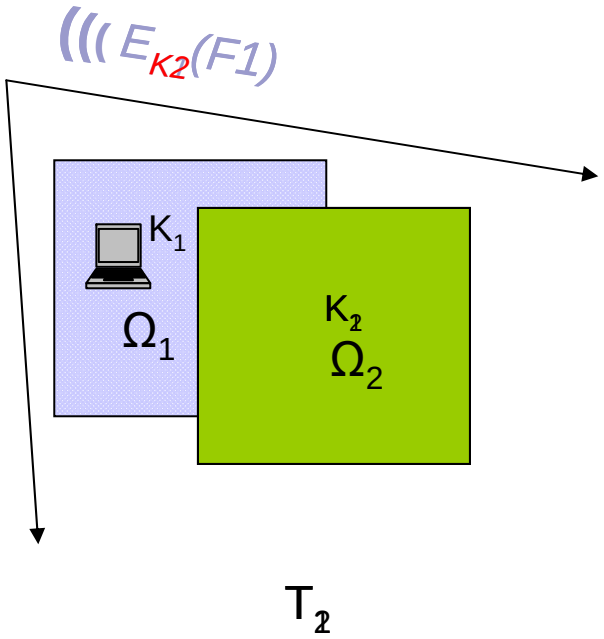
Dynamic Encryption

Question: Is static encryption enough to protect an object?

1. Object is streaming

2. Object's secure ST-region is temporal related





Dynamic Encryption

Solution:

- Decompose streaming objects
- Decompose ST-regions on temporal axis
- Use *dynamic encryption* :

  Encrypt objects with different keys at different time points
- Wireless nodes transmit the corresponding decryption keys at different time points.
- For stronger restrictions, we may need assistance from the OS! (e.g. once you have decrypted the file, you can always decrypt it!)

Another Problem :

- *How do we let the wireless nodes update the keys?*
- Do we issue updated keys to each node every time the key needs to change?

  Significant overhead! Future Research!

Summary

- Examined the new class of location based services---Spatio-Temporal Access Control (STAC).
  - STAC model
- Proposed the Seamless Feeding Architecture to support STAC
  - Algorithm for Optimizing the covered region
  - Dynamic Encryption
- Our mechanism:
  - Reduces the risk of privacy breach,
  - Resistant to Positioning Spoofing,
  - Facilitates new classes of applications with little effort.
    - Spatial-temporal scavenger hunt