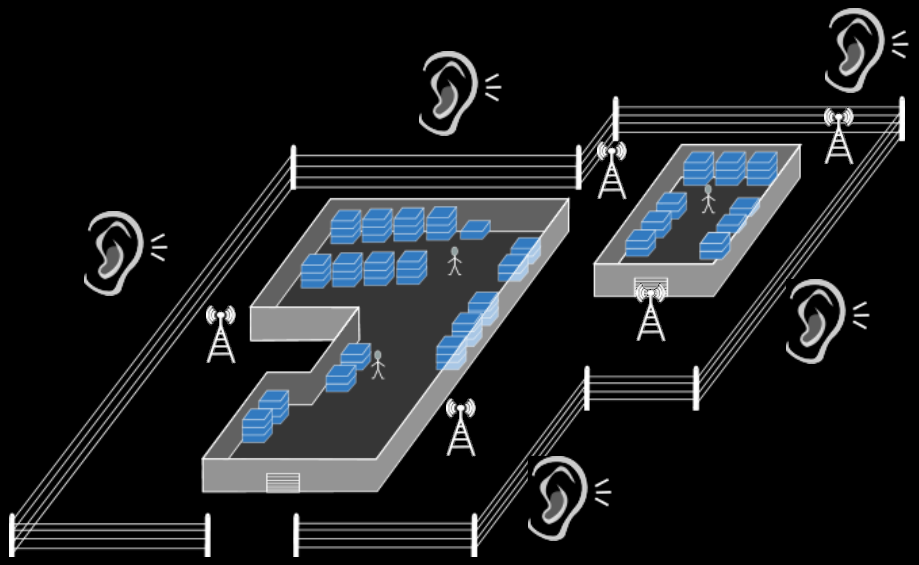
# Protective Jamming

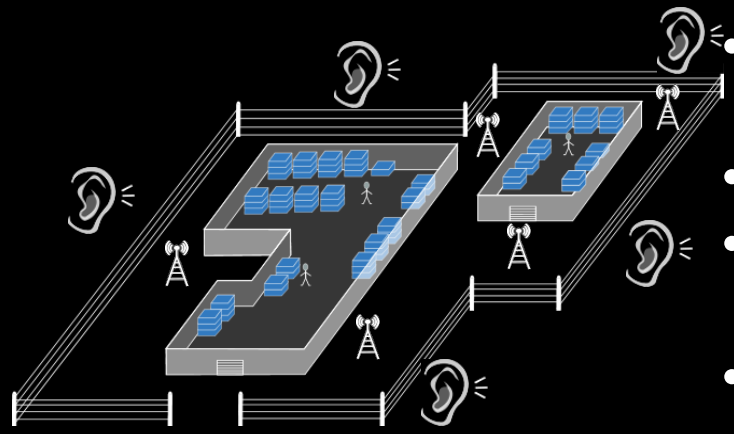
- S.Sankararaman, K. Abu-Affash, A. Efrat, E. Arkin, Y. Cassuto, J. Mitchell, S. Eriksson-Bique, V. Polishchuk, S. Ramasubramanian, and Michael Segal
- Started at 2012 and continues …



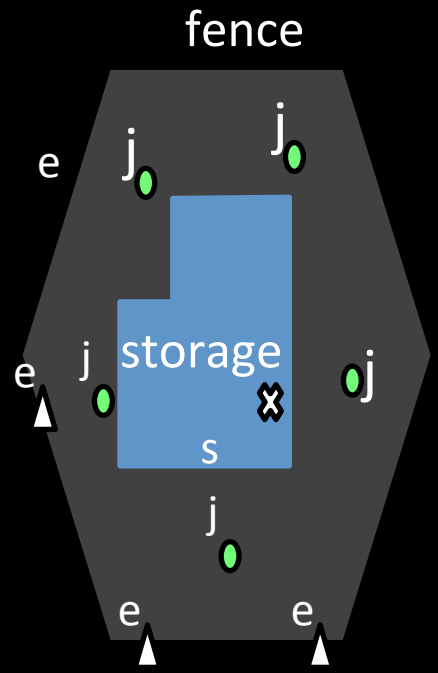
# RFID Devices

- Tags and Readers
- Sensitive information
  - Credit cards, patient information in hospitals, etc.
  - Tricky to encrypt due to severely limited capabilities

# Eavesdroppers and Jammers



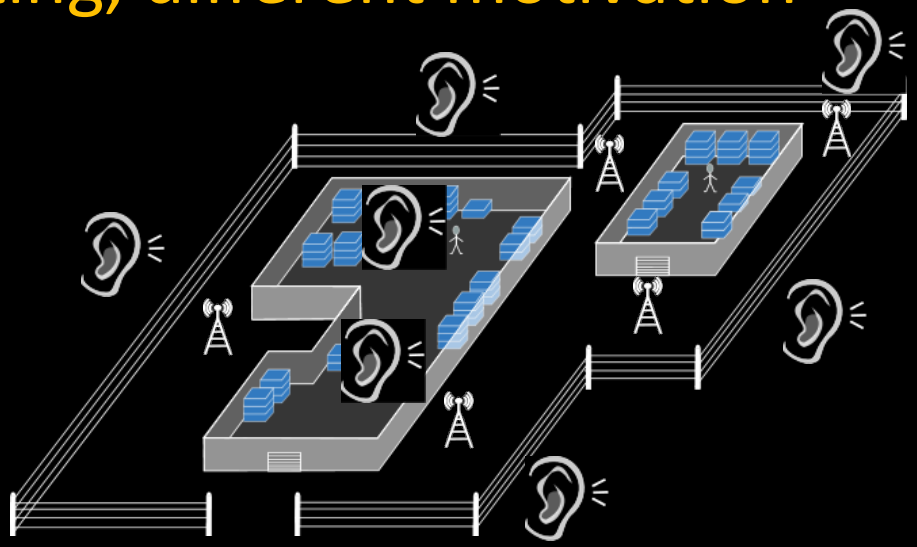
- RFID tags (or other active wireless sources), are placed in storage areas.
- The storage is surrounded by a fence
- Hostile eavesdroppers might be present outside fence.
- Idea for protection: Place (friendly) jammers that create "enough" noise to prevent successful unfriendly reading.
- This jamming should not disturb legit reading within storage.




Questions:

1. How to model successful jamming ?
2. Where to place jammers ?
3. Power assignments ?
4. How to orient antennas (if not omnidirectional) ?
5. How to schedule jammers (eg when battery operated)

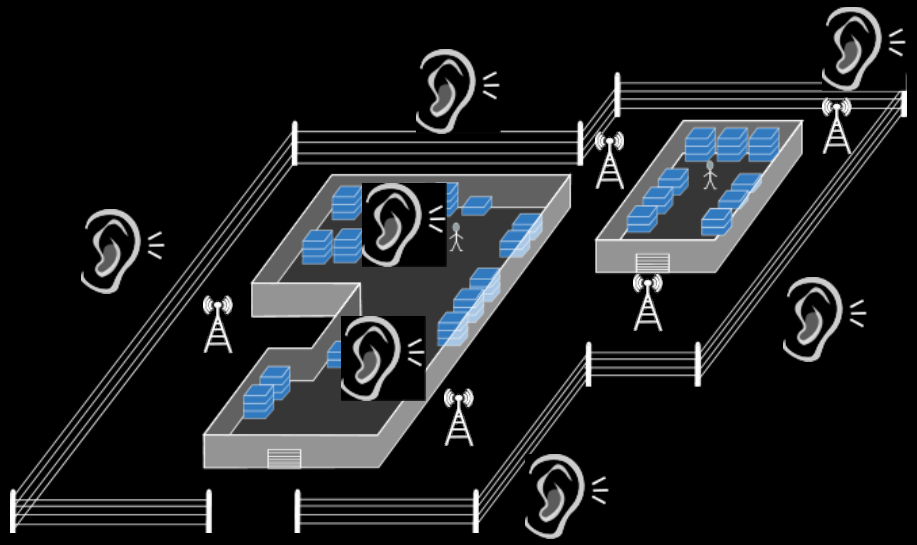
# Same setting, different motivation



- Inmates/Terrorists/Drug Dealers (depending on funding agency) inside a prison might (illegally) have cellphones
- Need to jam their communication with outside world, without disturbing legit users outside the (outer) fence of the prison.

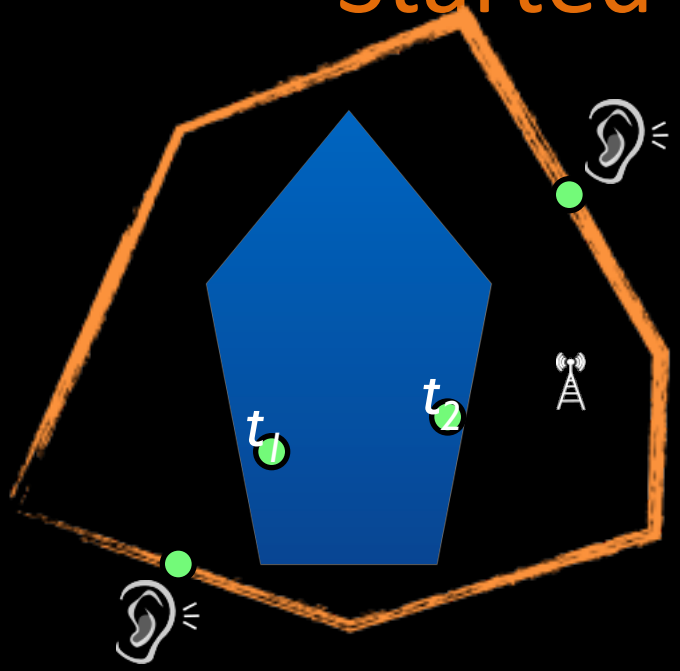
So jammers create virtual Faraday cage

# Same setting, yet another motivation



- Sensors communicate inside a sensors field.
- Eavesdropper outside the fenced region try to decrepit the sensor communications.
- Friendly jammers provide another level of security, on top of encryption.

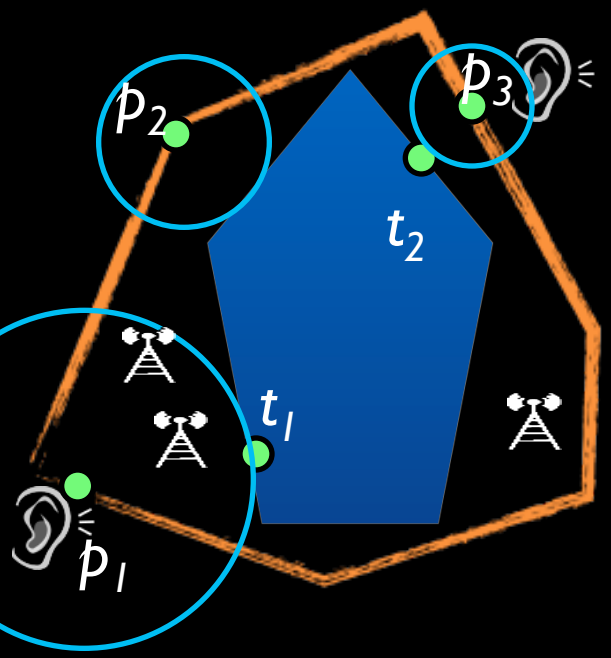
# Started with Assumptions




1. Only single frequency
2. Eavesdroppers could be anywhere outside fenced region.
3. No assumption about sensitivity of readers and eavesdroppers.

   => No assumptions about **range** of tags and jammers.
4. No co-transmissions from tags.
5. Jammers have no sensing abilities.
6. Other source of noise are not taken into account in SINR model (only simplify the problem)

# Successful Jamming




Def: Given user-specified thresholds $P_0$, $\delta_0$ jamming is *successful* if:

①For every point $t_i$ inside the storage, the summed power from all jammers < $P_0$.

②For every point $p_i$ outside the fence (possible eavesdropper), and every placement of RFID tag $t_i$, we have

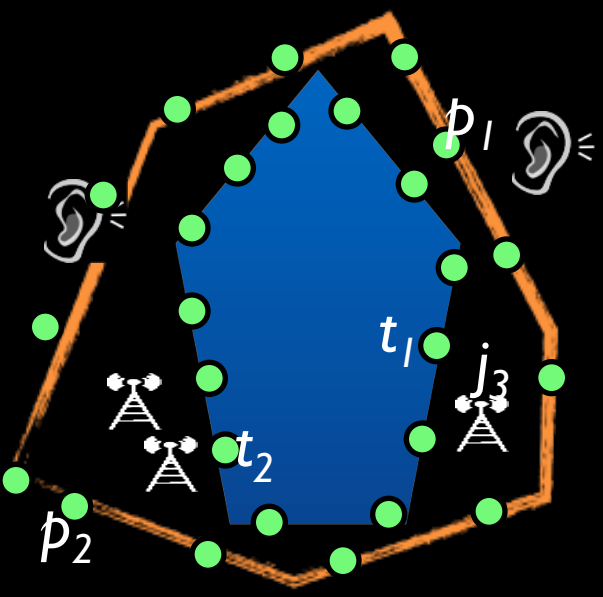
$$\frac{\text{Power received at } \boldsymbol{p_i} \text{ from } \boldsymbol{t_i}}{\sum_{j_k \in \text{Jammers}} \text{Power received at } \boldsymbol{p_i} \text{ from } \boldsymbol{j_k}} \leq \delta_0$$

Power received = power transmitted / distance$^2$

**Observation:** For every eavesdropper ***q***, need to worry only about nearest storage point (in omnidirectional case)

**Claim**: Under "reasonable" assumption, enough to validate conditions only for points on **boundaries** of fence and storage (jammers could be placed anywhere, though)

# Discretization, Witness Points




We could discretize the fence and storage boundaries by placing a set *W* of "*witness* points", and validate the conditions only on these points.

For every storage witness point

$$\sum_{j \in \text{Jammers}} \frac{\text{Power of } \boldsymbol{j_i}}{\text{dist}(t_i, j_i)^2} < P_0$$

For every fence witness point

$$\delta_0 \sum_{j \in \text{Jammers}} \frac{\text{Power of } \boldsymbol{j_i}}{\text{dist}(p_i, j_i)^2} \geq \frac{\text{Power of } \boldsymbol{t_i}}{dist(p_i, t_i)^2}$$

Conclusions: Can use it to `solve' variants of the problem such as

- Picking a subsets of jammers from candidate locations
- Schedule activation/deactivation of jammers activate to last longer.

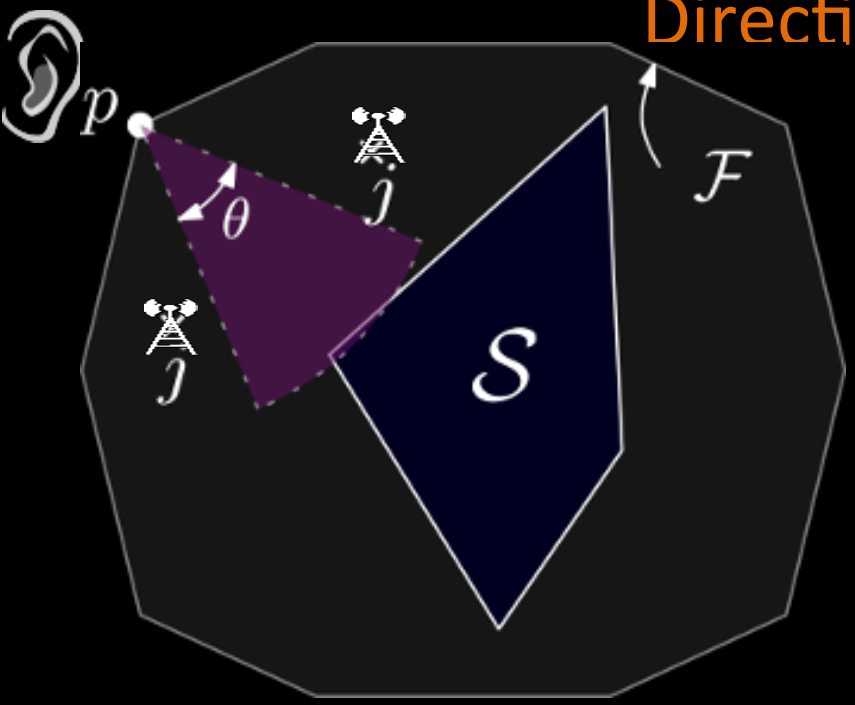
PROBLEM:

•Running time depends critically on #constraints, so could not use too many witness points. So challenging to provide guarantees for non-witness points.

New Result:

•Can place place only O(*n*/ε log (perimeter) ) witness points so successful is guaranteed everywhere, with ε-approximation of constants $P_0$, $\delta_0$

# Directional eavesdropper

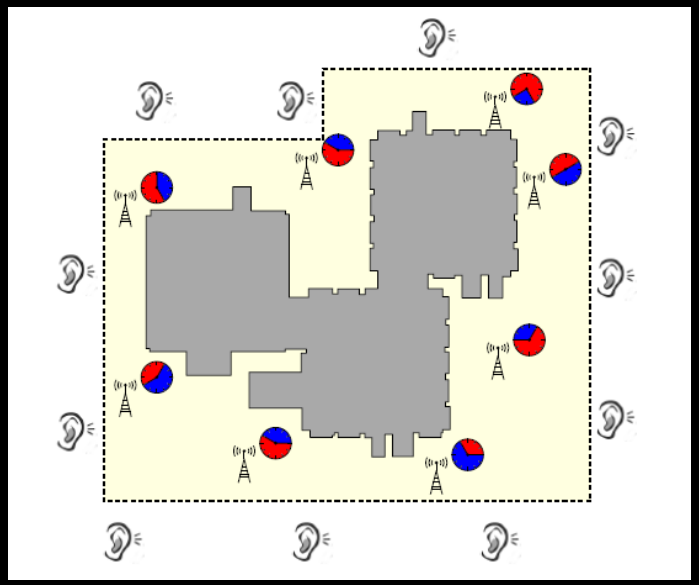



- Eavesdropper could try to avoid the noise from Jammers by using directional antenna
- Jamming problem now is to verify that for every **placement** and **orientation** of cone, successful jamming is obtained when considering only nodes within this cone
- The angle θ cannot be too small since RFID frequencies is usually 30Mhz
- Can show: # witness points is still bounded from above by

  $O(n^3/\varepsilon^3 \log(\text{perimeter}))$

# Extensions

- Spatial separation: different frequencies, different times



- Temporal jamming: try to jam selected bits, not all of them
- Bring geometry into account
- Problem becomes simpler if jammers using the same power

# Thank you