# Securing Wireless Data Networks against eavesdropping using smart antennas

Sriram Lakshmanan, Cheng-Lin Tsao
Raghupathy Sivakumar and Karthikeyan Sundaresan

Presenter: Zhenyun Zhang

GNAN Research Group
Georgia Institute of Technology

# Outline

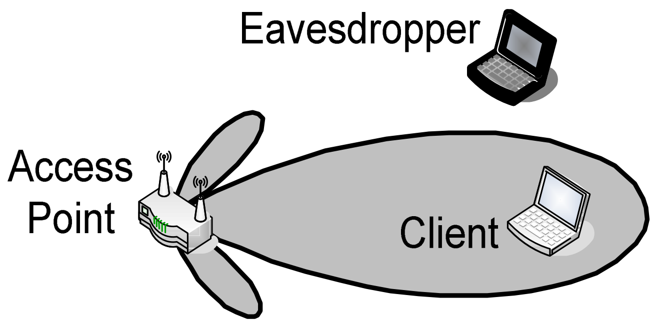
- Introduction
- Scope and Background
- Motivation
- Basic Techniques and Integrated Solution
- Performance Evaluation
- Conclusion

# Introduction

- Wireless Security:
  - Explosive growth of wireless data networks has led to increasing attention on specifically securing the wireless network
  - Wireless security solutions like WEP are dominantly cryptography based and typically extensions from their wired counterparts
- Scope of this work :
  - Using smart antennas to limit the knowledge of existence of information from an eavesdropper
  - A complimentary approach to cryptography based techniques

# Scope and Background

- A set of APs and Eavesdroppers M
  - APs have k elements, M have up to k elements
  - M have location information of clients and APs
- Exposure Region
  - Region in which eavesdropper can decode the signal




- Smart Antenna Beamforming
  - Adaptive arrays enable amplitude and phase weighting to obtain large set of antenna patterns
  - A k-element array at the transmitter (receiver) can place k-1 nulls in its pattern and control where it causes (receives) interference
  - When more than k parallel transmissions happen within an interference range, all transmissions become undecodable

# Motivation

- Why not just cryptography?
  - Actual solutions are not as secure as the core cryptographic scheme due to Implementation flaws, inability to realize true random numbers
  - Several unique privacy and targeted Denial of Service attacks due to the wireless channel not addressed by cryptography
    - Passive attacks like user fingerprinting * and active attacks like beacon attacks
- Why not just Line Of Sight beamforming?
  - Diminishing benefits with indoor fading, number of elements
  - Cannot handle non-contiguous security regions
  - Sub-linear exposure region with number of elements
- *Can an intelligent scheme achieve larger security benefits?*

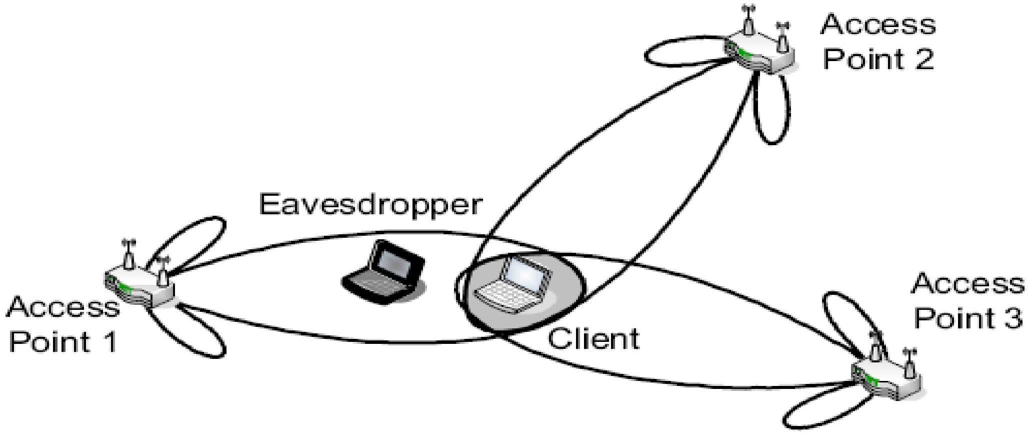


* 802.11 user finger printing, Jeff Pang et al, ACM Mobicom 2007

# Virtual Array of Physical Arrays

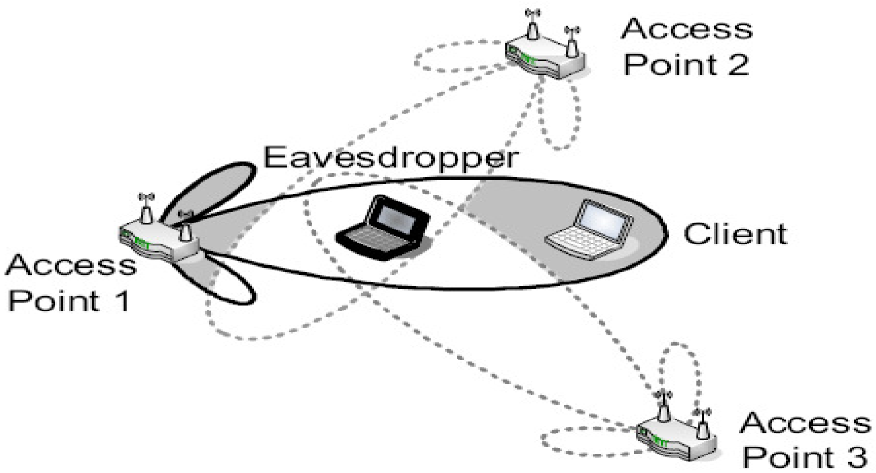
- Setting
  - Enterprise WLAN with central controller that coordinates decisions of p APs (Virtual array)
  - Each AP has a k element array (physical array)
- Basic strategies
  - Information deprivation – prevent eavesdropper from getting access to the required information/signal
    - Secret sharing
  - Information Overloading – overload eavesdropper with more signals than it can sustain
    - Controlled jamming
    - Stream Overwhelming

# Secret Sharing



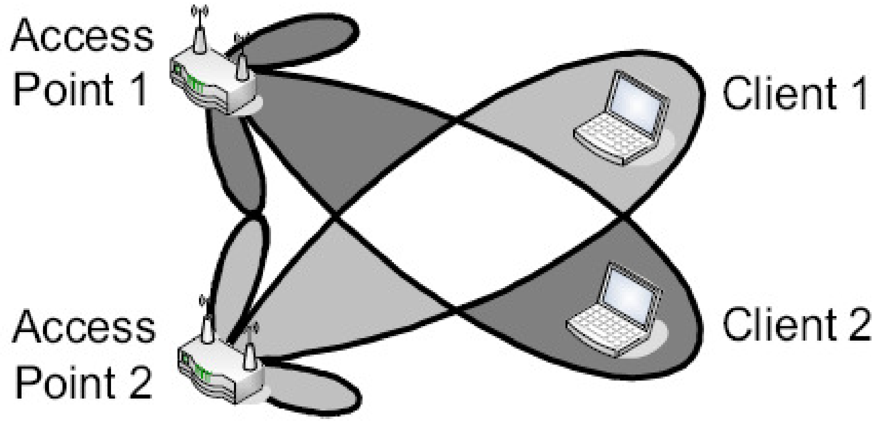

- Idea:
  - Create t' shares of the message such that all shares are required for decoding the message
  - Transmit the shares through different APs by leveraging the high density of access points reachable from each client
  - While client receives all shares, eavesdropper does not receive all shares and cannot decode the message

# Controlled Jamming



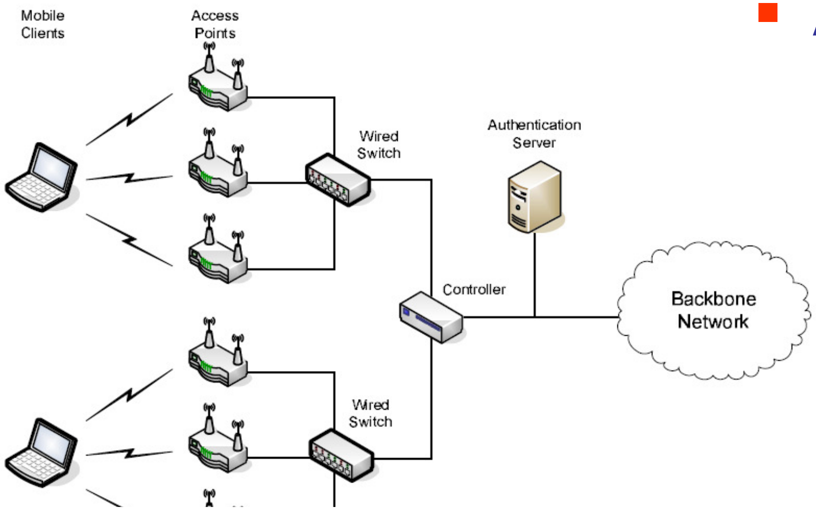

- Idea:
  - Use the available Degrees of Freedom (elements) at an AP to jam areas in the network except around the desired clients
  - APs suppress interference to desired clients by adapting their beams
  - Use in conjunction with the maximum allowed power to prevent access in locations without authorized clients
  - Eavesdropper needs to suppress interference from each element of the active APs (p'*k) in the vicinity to thwart this scheme

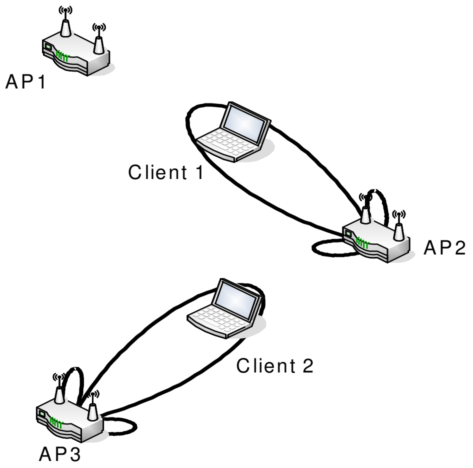
# Stream Overwhelming




- Idea:
  - Choose AP- client pairs such that overlap of the data streams causes poor decodability
  - Except around the clients, many other areas are overwhelmed
  - APs exploit transmit side interference  suppression to protect clients whereas the eavesdropper is overloaded
  - Eavesdropper overloaded by coordinating data transmissions (as opposed to transmitting jamming signals in the previous case)

# Integrated Operations




- Architecture
  - Central controller which controls transmission of each AP
  - Transmissions are synchronized
  - Downstream and upstream communication alternate in epochs
  - Controller knows the location of APs and approximate location of clients
- Operation
  - For a given throughput constraint, if security is to be maximized,
  - *A combination of stream overwhelming and secret sharing (with preference to secret sharing) should be used,*
  - *The remaining APs devoted to controlled jamming*

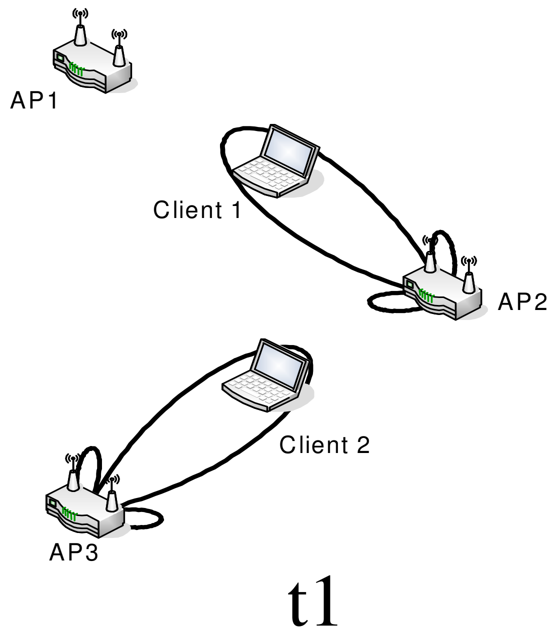
# Algorithms and Implementation

- Two cascaded schedulers
  - Throughput scheduler
    - Input:  S parameter, connectivity matrix, packet sequence
    - Output: S' In-sequence  packets out of the first S packets
    - For each AP determine the number of clients in the stream
    - Greedily assign packets in-sequence by assigning the client to the AP with minimum APs
    - Update the APs and the Degrees of Freedom
  - Security Scheduler
    - Input: S', packet sequence, connectivity matrix
    - Output: Action for each Ap in each fragment duration
    - For each fragment m and each AP determine availability
    - Sort the APs in ascending order of available fragments
    - Greedily assign APs and update the DOF
    - Adjust for stream-overwhelming
    - Assign remaining APs for controlled jamming while ensuring already assigned clients remain unaffected

# Algorithm Illustration


| AP \ timeslot | t1 | t2 |
|---|---|---|
| AP1 | J | $C1_2$ |
| AP2 | $C1_1$ | $C2_2$ |
| AP3 | $C2_1$ | J |

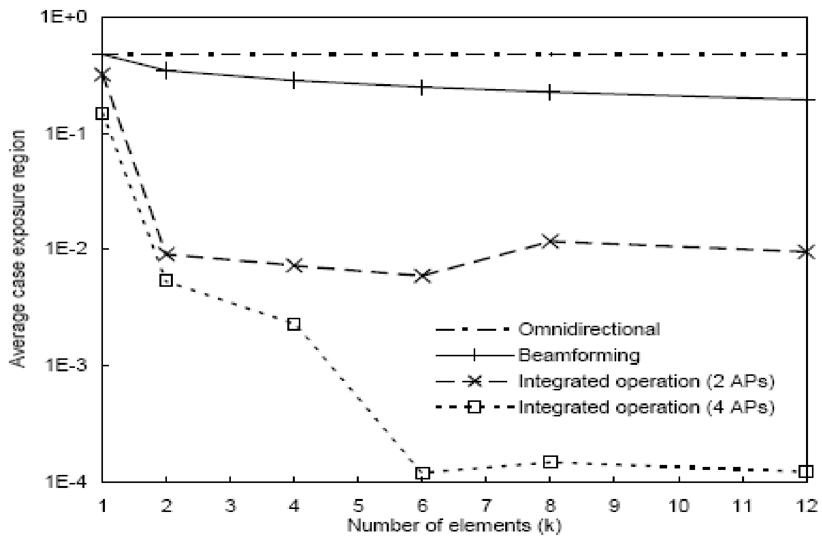
AP-client association

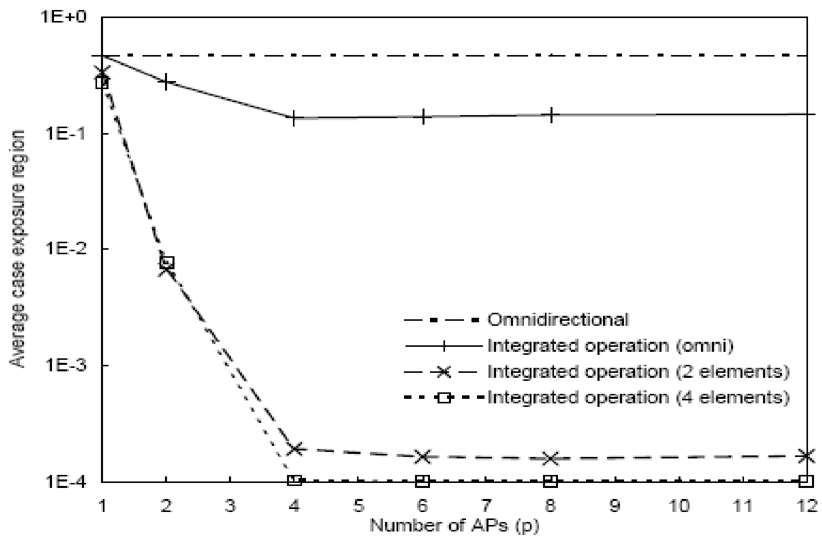


# Performance Evaluation

- Custom simulator in C++
  - Adaptive beamforming with interference suppression
  - Channel modelling
    - ITU Indoor attenuation model with a path loss exponent of 4 and lognormal fading with a standard deviation of 2.5dB
    - Link fade margin of 3dB with operating frequency of 2.4 GHz
    - SNR threshold of 15dB
    - Noise floor of -100 dBm, Rx. sensitivity of -85 dBm
    - Transmission power of 20dBm
  - Random position of clients, eavesdropper and APs in a 100m * 100m grid
  - Default values of 20 clients, 4 APs, 4 array elements
  - Downstream flows to a random subset of clients
  - Metric: Average Exposure region

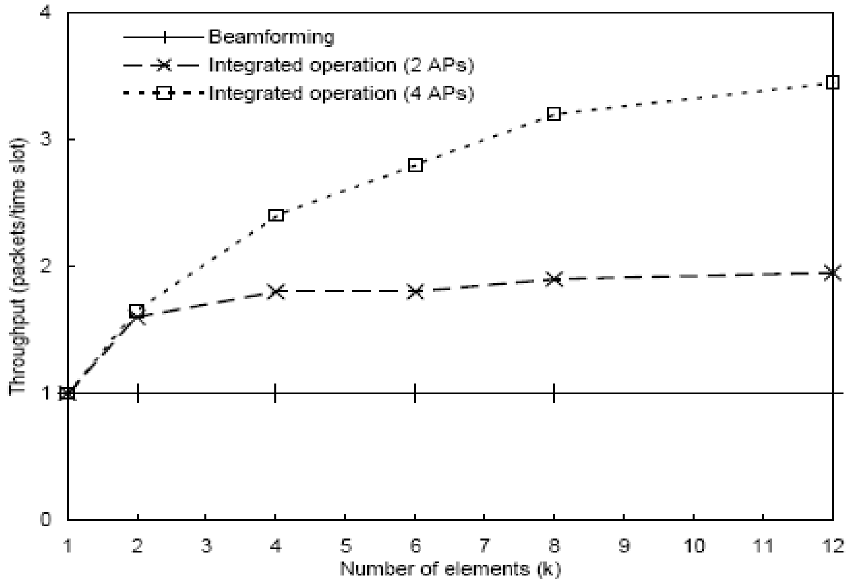
# Performance Evaluation (1/2)

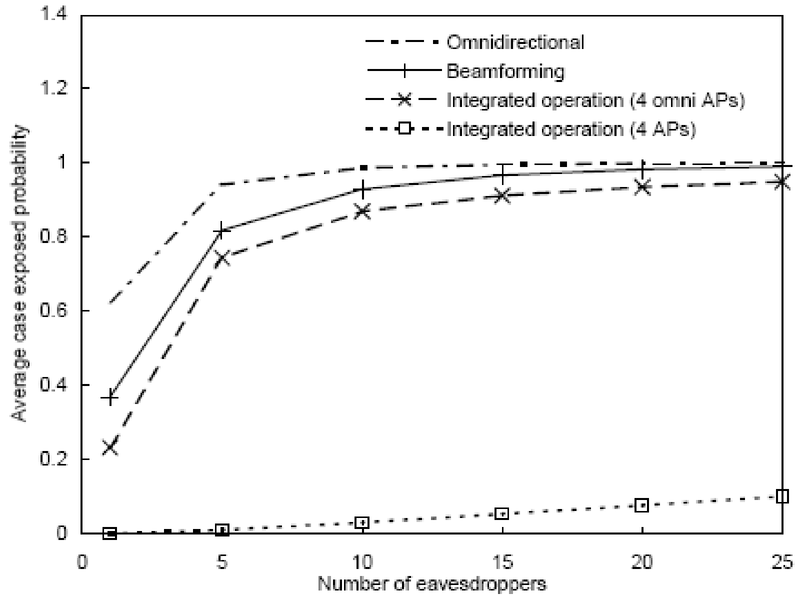



- With increasing k,
  - Beamforming security gives diminishing returns
  - Integrated algorithm provides large reduction in security with an example exposure region of 1% with just 2 elements and 2 APs.
- With increasing p,
  - Improvements are much larger because of the large secret sharing possibilities
  - With 4 elements and 4 APs, exposure region reduced to 0.01%

# Performance Evaluation (2/2)




- Throughput is preserved by the algorithm due to intelligent use of resources
- Eavesdropper collusion affects the integrated algorithm to a much smaller extent when compared to omnidirectional and beamforming
- Slight increase of exposure probability (but less than 10%) when the number of colluding eavesdroppers is increased upto 25

# Conclusion

- Summary
  - introduced the idea of using spatial smartness to provide security against eavesdropping
  - presented three novel mechanisms that fundamentally improve security against eavesdropping
  - evaluated the performance of an integrated algorithm that uses the three mechanisms in tandem, using simulations
- Future work
  - Implement the solutions in an actual environment  with appropriate prototypes
  - Study the details of the beamforming algorithm in indoor settings considering complexity
  - Study the security vs throughput trade-off in detail

Thank You

For further details:

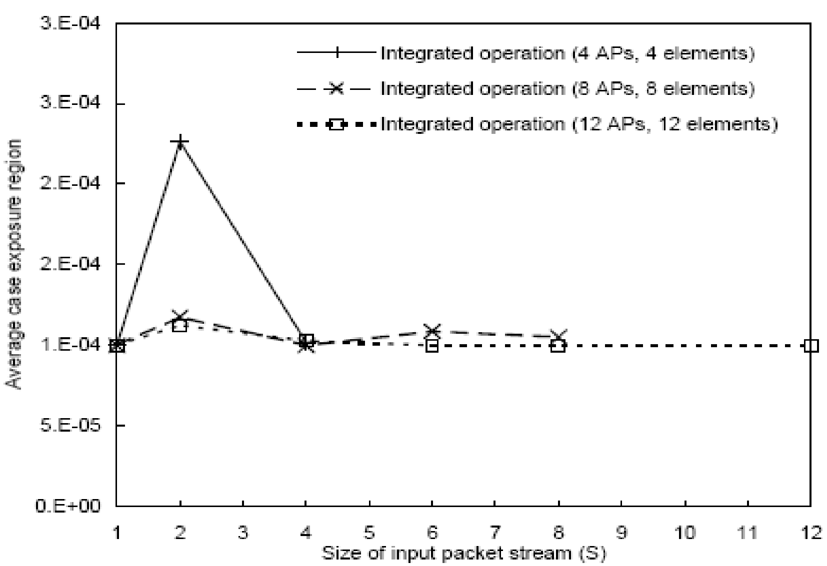
www.ece.gatech.edu/research/GNAN
/archive/2008/icdcs08a.html

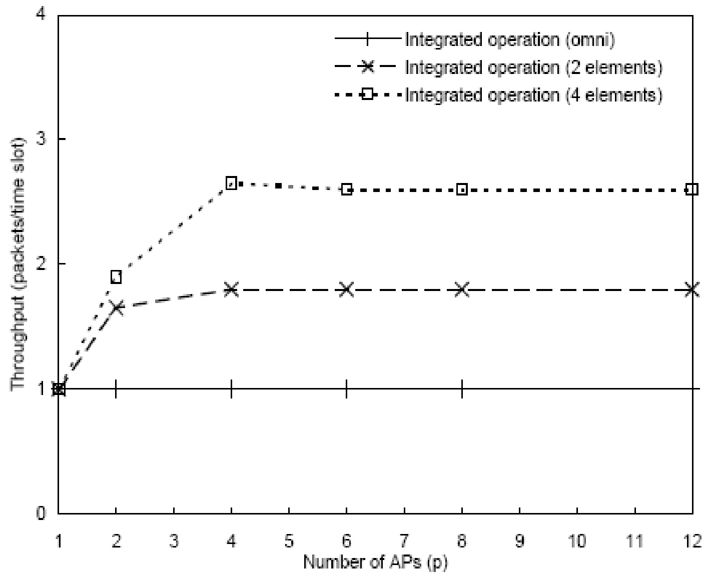
Email feedback/comments to:

sriram@ece.gatech.edu

# Performance Evaluation - backup

- When rate parameter is changed, the exposure region slightly increases and then decreases since as S increases both the number of packets scheduled and the possibility of separated clients increases.
- When the number of APs is increased, the integrated algorithm gives increased benefits which saturate when possible spatial reuse in the network is exhausted.

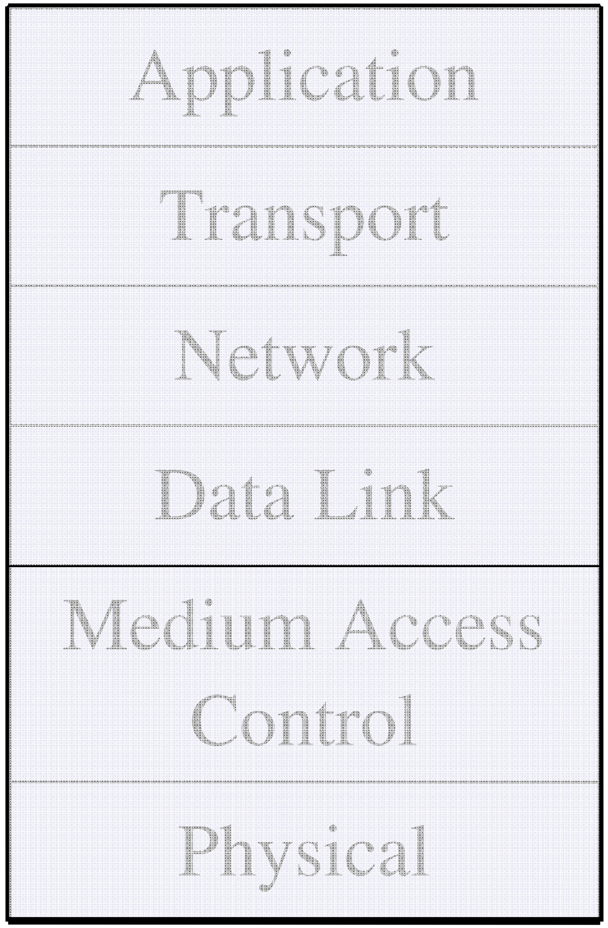


# Difference between cryptography and smartsec

- Encryption
  - Disclosing the signal
  - Hiding the message in the signal
  - Data-link layer or above
  - Relies on computational complexity
  - Cannot prevent unique security attacks due to wireless broadcast nature such as fingerprinting
- Our approach
  - Hiding the signal
  - Physical or MAC layer
  - Smart antennas
  - Relies on spatial and channel conditions which are less controllable by eavesdropper

TCP/IP protocol suite



# Quantitative Results

| Strategies | Exposure region (m^2) |
|---|---|
| Omni-directional | 1725.46 |
| Beam-forming | 855.69 |
| Secret Sharing | 146.55 |
| Controlled Jamming | 23.74 |
| Stream Overwhelming | 232.86 |
| Integrated | 5.69 |

# Simulation Parameters

| | |
|---|---|
| Max tx power | 20dBm |
| Sensibility | -85dBm |
| Noise | -100dBm |
| SINR threshold | 15dB |
| Frequency | 2.4GHz |
| Path loss factor | 4 |
| Link margin | 3.2 dB |
| Number of APs | 4 |
| Number of elements | 4 |

# All or Nothing encryption

- Procedure such  that all shares must be recovered to recover the message else there is  no information disclosure
- Developed  by R.L.Rivest
- Lecture Notes in Computer science,volume 1267, issue 210, 1997
- Involves xoring the fragments each of which is X bits by dividing the total packet into fragments of size X bits

# Why 3 schemes

- There are two flavours of approaches namely deprivation and overload
- For these, capacity preserving and capacity sacrificing techniques can be found
- While deprivation leads to directly a capacity preserving scheme such as secret sharing
- Overload has two flavours to adapt to network conditions
- The controlled jamming and stream overwhelming are the 'extreme' techniques in the range of overload techniques
- Thus for flexibility we include 3 schemes