**STUDY OF PHYSICAL LAYER SECURITY IN WIRELESS COMMUNICATION**

**Mustafa Duruturk**

**Introduction**

Talks about diversity systems. Multiple Transmitters. MIMO, also called Multiple Antenna systems or Smart Antenna systems, how they help in beam forming for pointing signal in a specific direction.

Adaptive arrays can steer the beam at a point of interest and also know about the interfering signals. Smart Antenna systems are mostly adaptive arrays.

**Wireless Security Systems**

WEP: Wired Equivalent Privacy, Its improvements and weaknesses

Two aspects of wireless security:

Authentication: achieved with MAC Layer

Encryption: achieved with WEP

**Problem with Auth using MAC:**

* MAC can be changed
* Hardware dependent and hardware can be modified

**Problem with encryption using WEP**

* Easily decodable
* People use VPN as an alternative

**Some common wireless security problems**

* Easy Access
* Rogue Access Points
* Unauthorized use of service
* Denial of service attacks by saturating access point with connections and excess network traffic
* MAC spoofing and hacking: Attacker can use the same source MAC address along with same data frame and pretend to be the user
* Traffic Analysis and eavesdropping: Header frames can be captured and analyzed since they are not encrypted.

**Some security requirements**

* Encryption
* Rogue access point detection
* Sensitive data should not be transmitted over public networks
* Two-factor authentication
* Authentication should be hardware independent

**Security Layers**

* *Wireless LAN layer:* Lowest layer, directly deals with data. Sends out beacons and tracks connection attempts on network. Encrypts and Decrypts after successful connection.
* *Access Control Layer:* Responsible for contents of the data traffic. Ensures all the data in network is only from devices which are authenticated.
* *Authentication Layer:* Authenticates connections. Establishes user identity when connection is attempted. In Access point if n/w is small. In a dedicated server if n/w is big

Key based wireless security increases management overhead with increasing number of nodes in the network. The project analyzes the security performance provided by using a wiretap channel and a private key known only to the destination. **In short, there is no shared secret.**

**In order to achieve secure communications without any shared secrets, the designated receiver intentionally injects a noisy feedback during the sender’s transmission such that any message received at the eavesdropper has no clue about the source message from the sender.**