



New Avenues for Data Network Security

Aftab Ahmad

aftab@nsu.edu

Computer Science, [Norfolk State University](#)

[20 Oct. 2005](#)



Outline

Layered Network Architecture

Data Security Requirements

Current Security Mechanisms

Objectives for Solutions

Security Protocol Architecture

Common Data Security Network (CDSN)

Motivation for CDSN – Results from Wi-Fi

Future Work



Layered Network Architecture

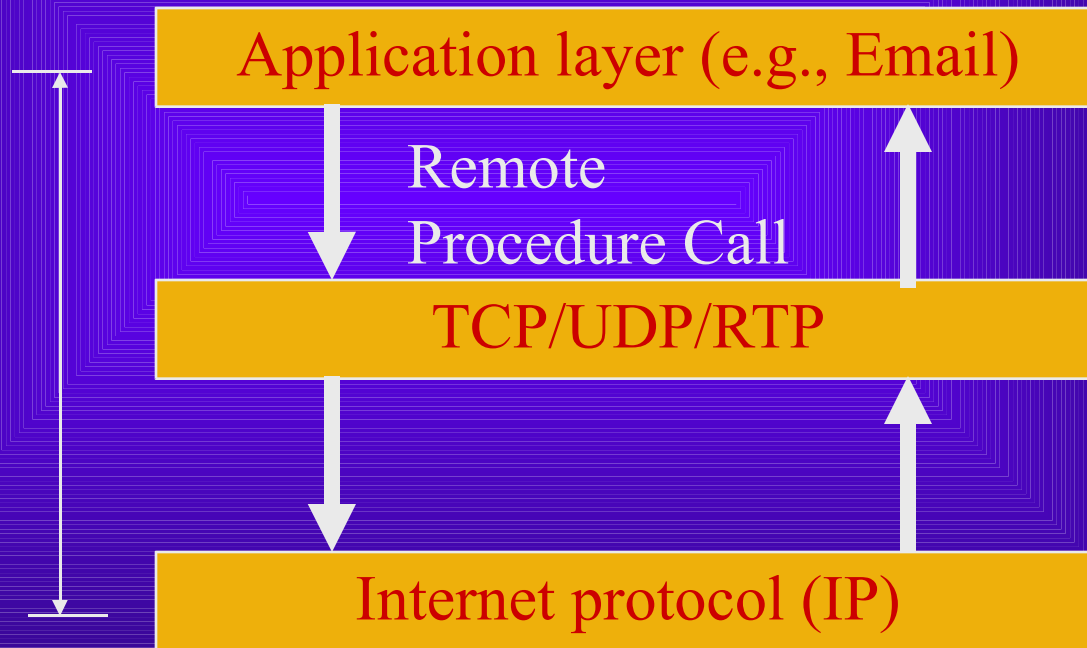
Such as the Internet

- Have layers of protocols
- Data passes through each layer
- Each layer adds protocol information
- Protocol information is meant for peer layers
- “Primitives” are used for passing information between adjacent layers

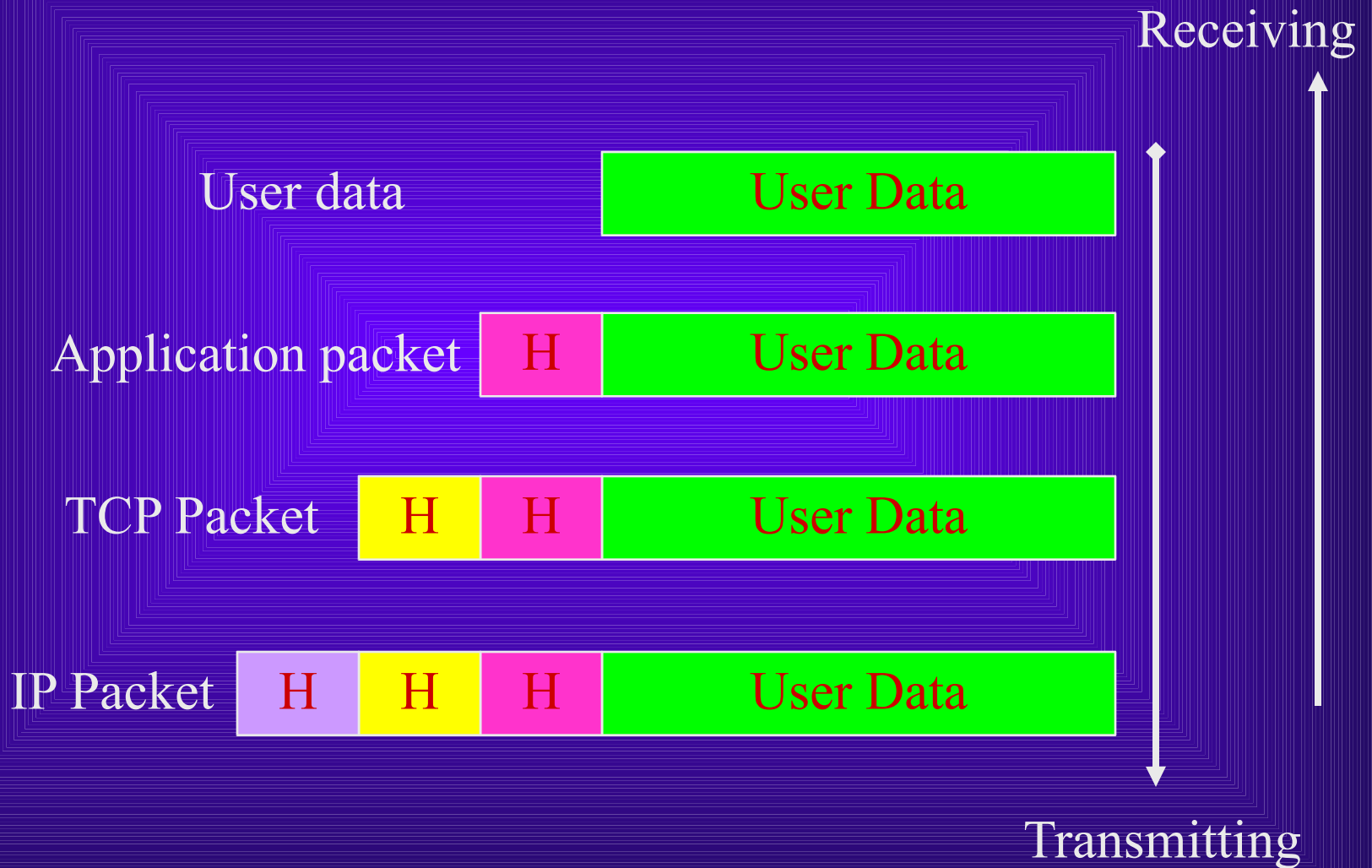
Most current networks follow this paradigm

Layered Network Architecture II

Socket



Layered Network Architecture III





Data Security Requirement

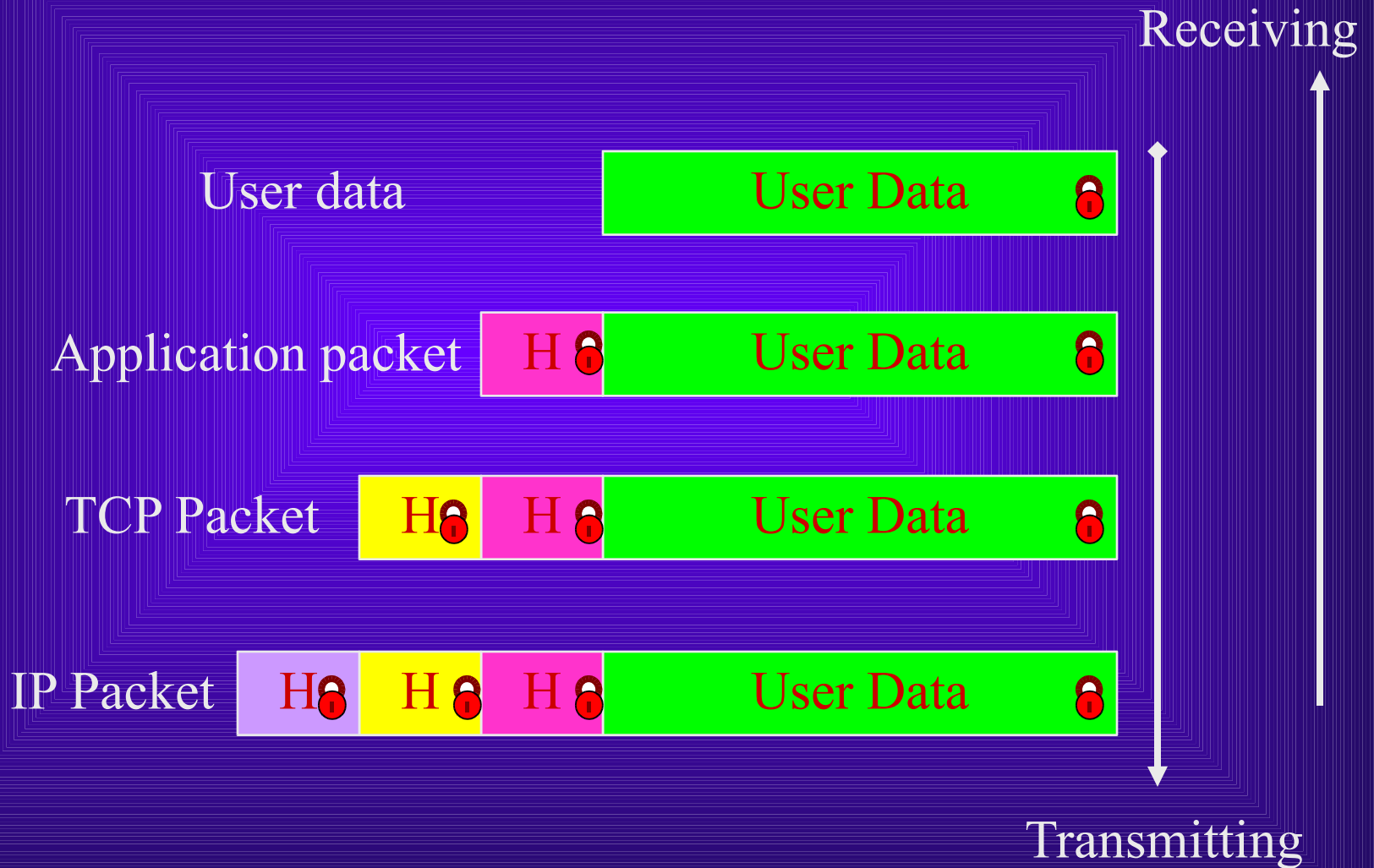
Each layer offers a security hole

In wireless networks, the medium itself is vulnerable

Security between IP layers does not guarantee security between TCP layers

That is why, we have security protocols on each layer: Certificates, Transport Layer Security (TLS), IPSEC, IEEE 802.11i

Data Security Requirement II



Data Security Requirement III

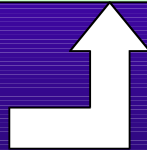
Malicious Reliability layer

Knows exactly what identifier is required to get a packet from routing layer. Receives the packet. Sending reliability layer assumes that the correct receiving reliability layer received it.



Secure Routing layer

Checks security, strips off the routing header and delivers packet to higher layer with a given identifier.



Packet arriving with
security guarantee



Current Security Mechanisms

Security set in isolation in each layer

A host (computer) must be configured to have security at each layer.

All layers have their own secure protocols

- In LDAP we set up permissions
- TLS for transport level (Secure Socket)
- IPSEC for IP layer (Header and ‘Payload’)

There is no real interaction between layers



Current Security Mechanisms II

There is a cost of security in terms of

- Transmission and Processing Delays

The Problem

- Security is affixed at each layer
- You always pay the cost whether you need the security or not
 - Most Internet surfing does not require security
 - Heterogeneity and laws add another dimension



Objectives for Solution

Security to be adaptive for applications

Automatic security mapping between protocol layers

- You set the security only at application level

Security does not depend on intermediate network



Security Protocol Architecture

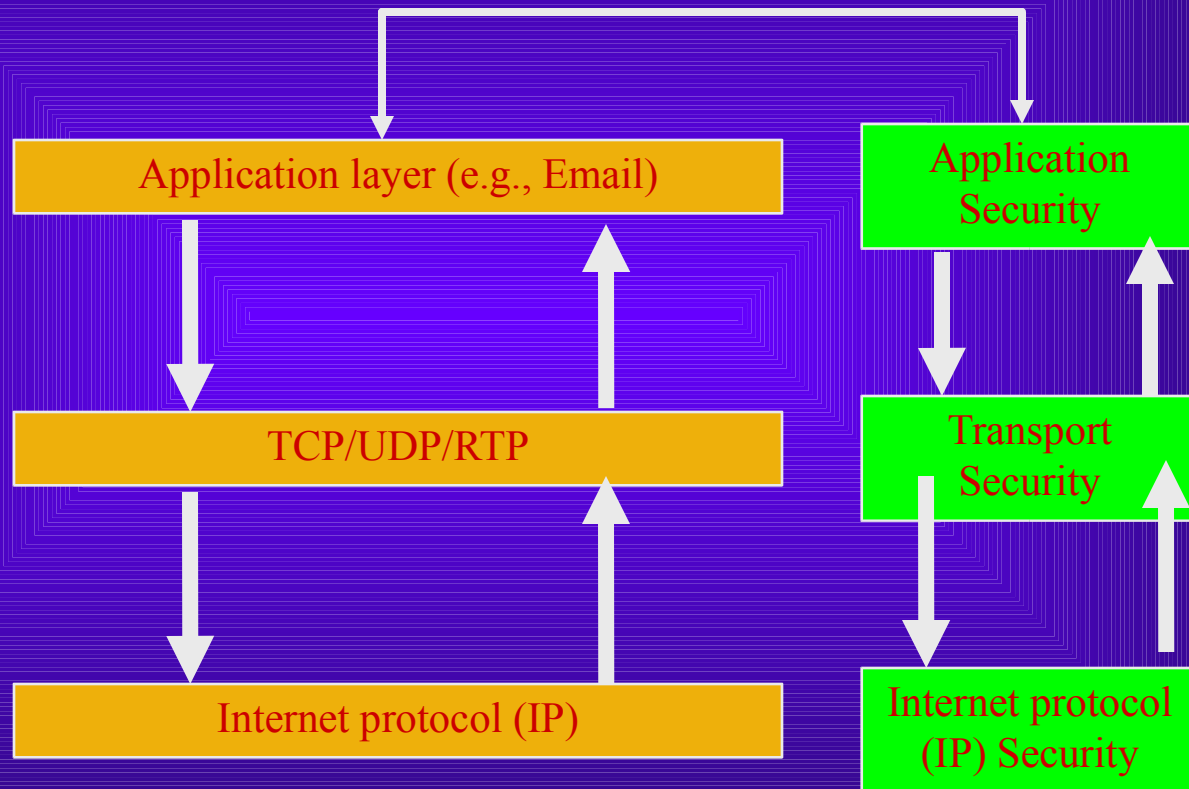
Layered model

One security plane for each protocol plane

If security specified at application level, no need of specifying it at lower levels

Each network can have a separate security architecture

Security Protocol Architecture II





Security Protocol Architecture III

Observation: Interaction between security and transmission protocols only at the application layer

Implication: Security set only end-to-end

Implication: How to ensure that security can be provided at intermediate networks

Solution: Keep security network independent of transmission network



Common Data Security Network

CDSN is a network independent of Internet

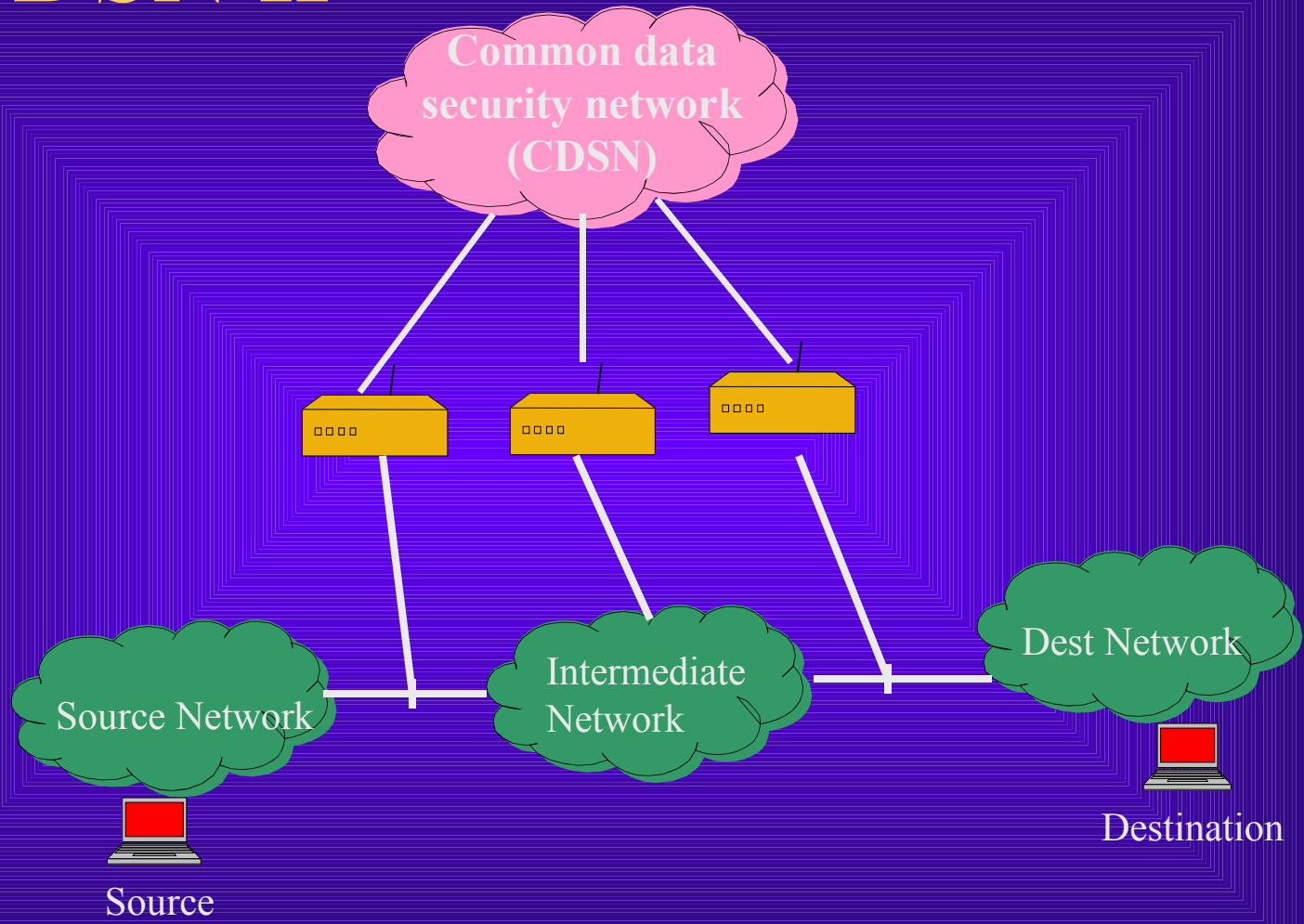
It does not carry user data

- It only implements security, end-to-end

Defines several types of nodes

- Security processing stations implement the requested security level
- Security check-points define the requested security in terms of the available resources

CDSN II





CDSN III

Security attributes and associations (SAAs) define the security profile requested by an application.

Security checkpoints (SCPs) extract SAAs and provide their values to SPS

Security processing stations (SPS) define new security filters for intermediate networks

Inter-layer mapping depends on architecture

CSDN IV

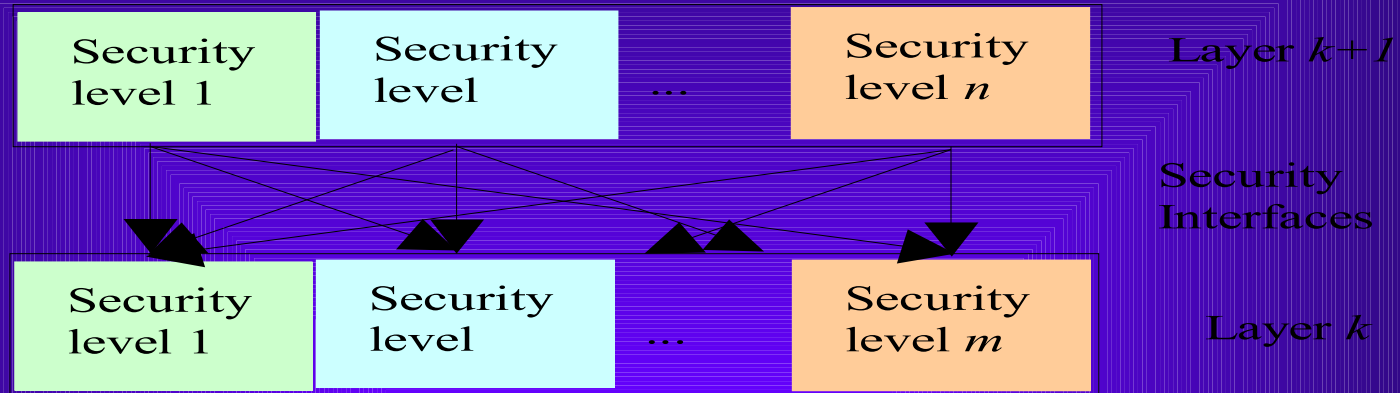


Fig. 3. Inter-layer security mapping.

Each layer can present a variety of scenarios

Many user profiles can be defined based on

- How much a user can pay



CDSN V

What is required

- Define scenarios at each layer and map them
- Define inter-layer communications
- Associate cost with each scenario

Scenario definition relatively simple

- IPSEC: No security, Authentication Header (AH), ESP, Certain Encryption suites, combinations (SPD, SAD, Selectors)

WLAN: No security, WEP, 802.11i



CDSN VI

Current work

- Scenarios and cost in WLANs
- Scenarios and cost in IPSEC

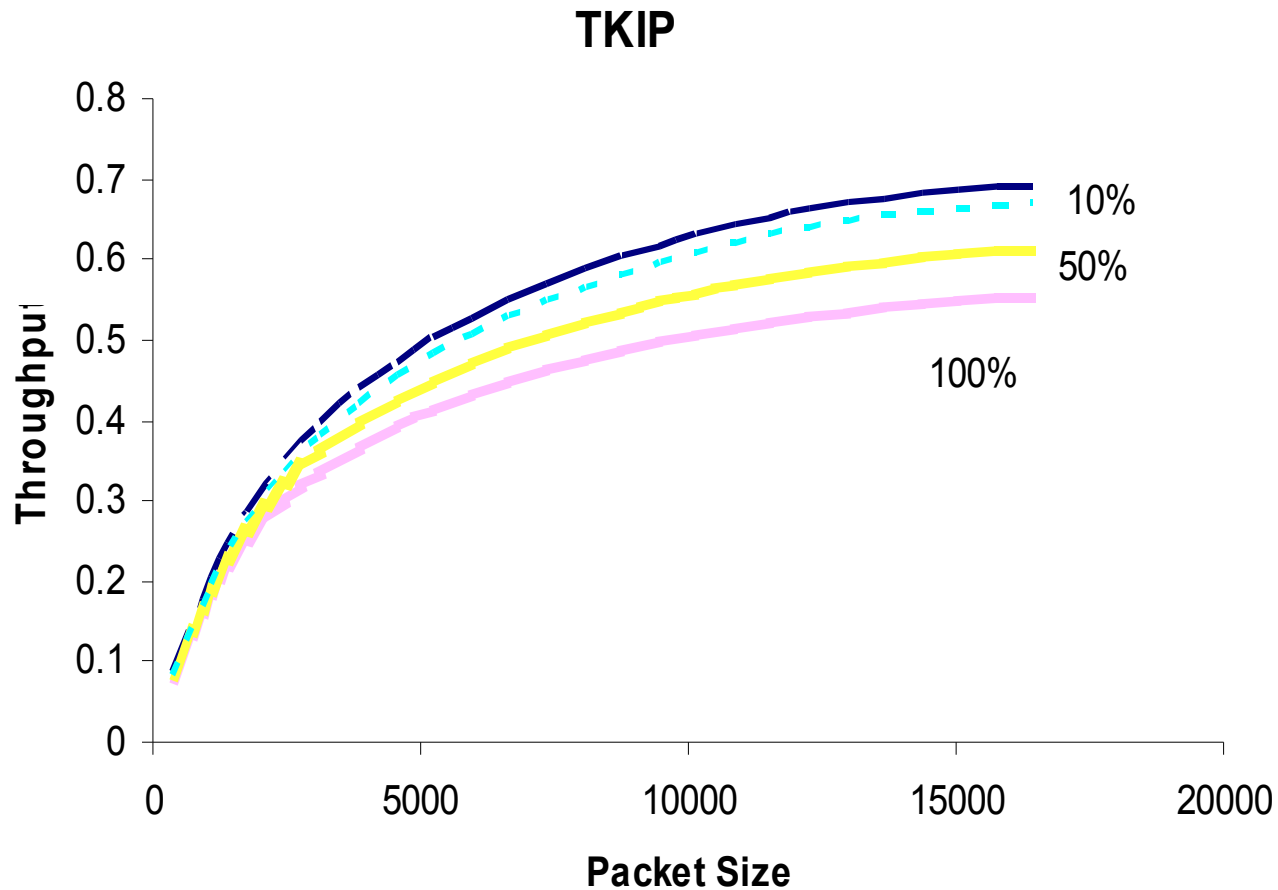
Major results

- IEEE 802.11i could be very costly
 - Especially the mandatory CCMP
 - Handoff could add significant overhead

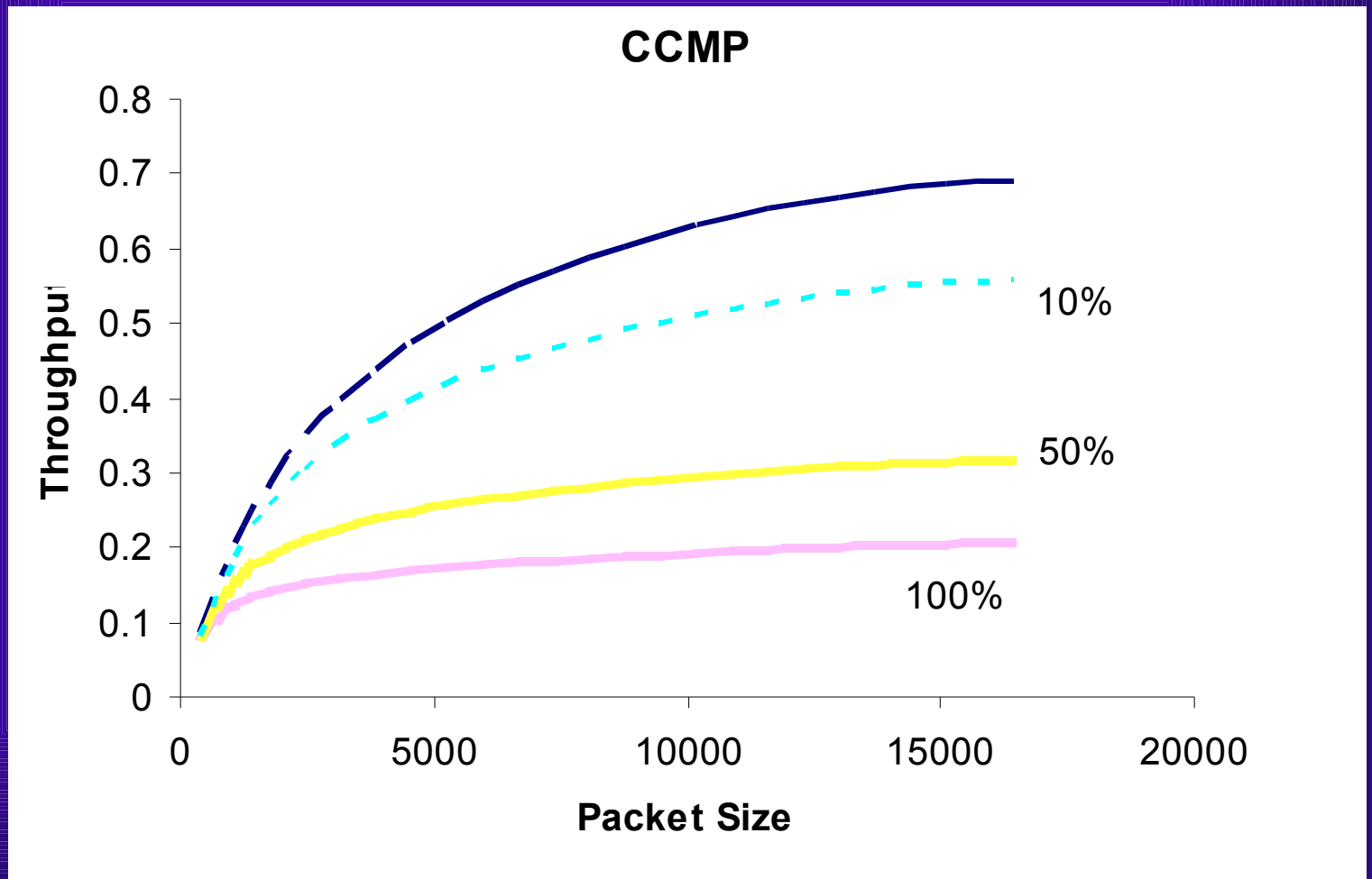
Next step

- Get more results about 802.11i and IPSEC
- Map IPSEC and IEEE 802.11i scenarios

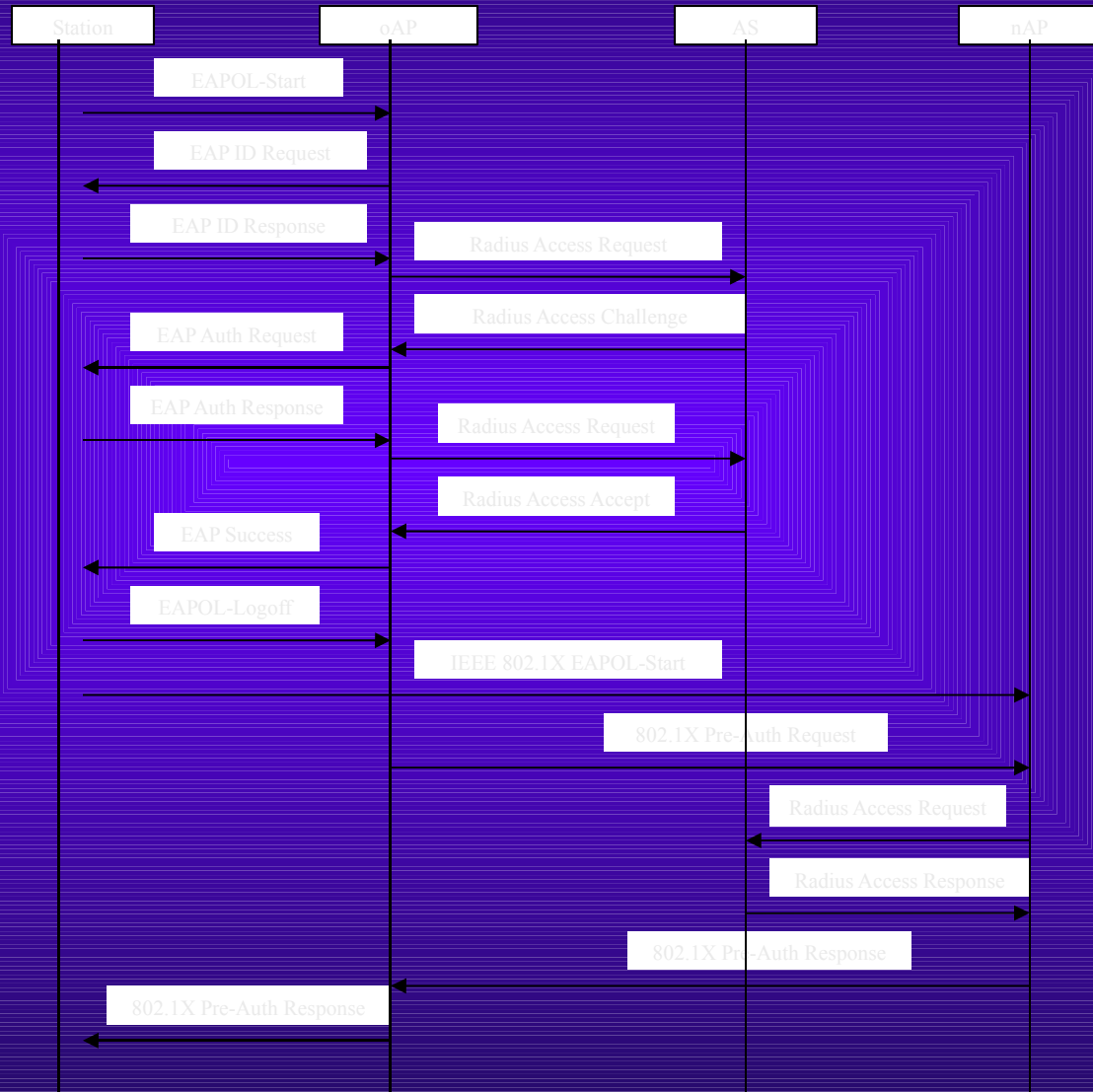
Reduction in Throughput using TKIP (WPA)



Reduction in Throughput Using CCMP (IEEE 802.11i)



IEEE 802.1X: Pre-Authentication Message Sequence





Future Work

Determine scenarios at transport and application layers

Map scenarios from Applications down to Physical layer

Define inter-layer communications mechanisms

Design an actual security architecture with adaptive security capability and possibly CDSN.