System and Network Security

Dr. Ashok Kumar Das

Center for Security, Theory and Algorithmic Research
International Institute of Information Technology, Hyderabad

E-mail: *ashok.das@iiit.ac.in*
URL: http://www.iiit.ac.in/people/faculty/ashokkdas
Personal Home Page: http://sites.google.com/site/iitkgpakdas/

Encrypting Communications Channels

Encrypting Communications Channels

- This is the classical Alice and Bob problem:
  Alice wants to send Bob a secure message.
- What does she do?
- She encrypts the message.
- In theory, this encryption can take place at any layer in the OSI (Open Systems Interconnect) communication model.

Encrypting Communications Channels

- In practice, it takes place either at the lowest layers (one and two) or at the higher layers.
- If it takes place at the lowest layers, it is called ***link-by-link encryption (LLE)***; everything going through a particular data link is encrypted.
- If it takes place at higher layers, it is called ***end-to-end encryption (EEE)***; the data are encrypted selectively and stay encrypted until they are decrypted by the intended final recipient.

Layer-wise Network Security Protocols

Datalink Layer: Security protocols for proving the error detection mechanisms due to bit transmission error and bits changed by an adversary (intruder) in between the communication

- Internal Error Control
- External Error Control

Layer-wise Network Security Protocols

Network Layer: Internet Security Protocol (IPSec)

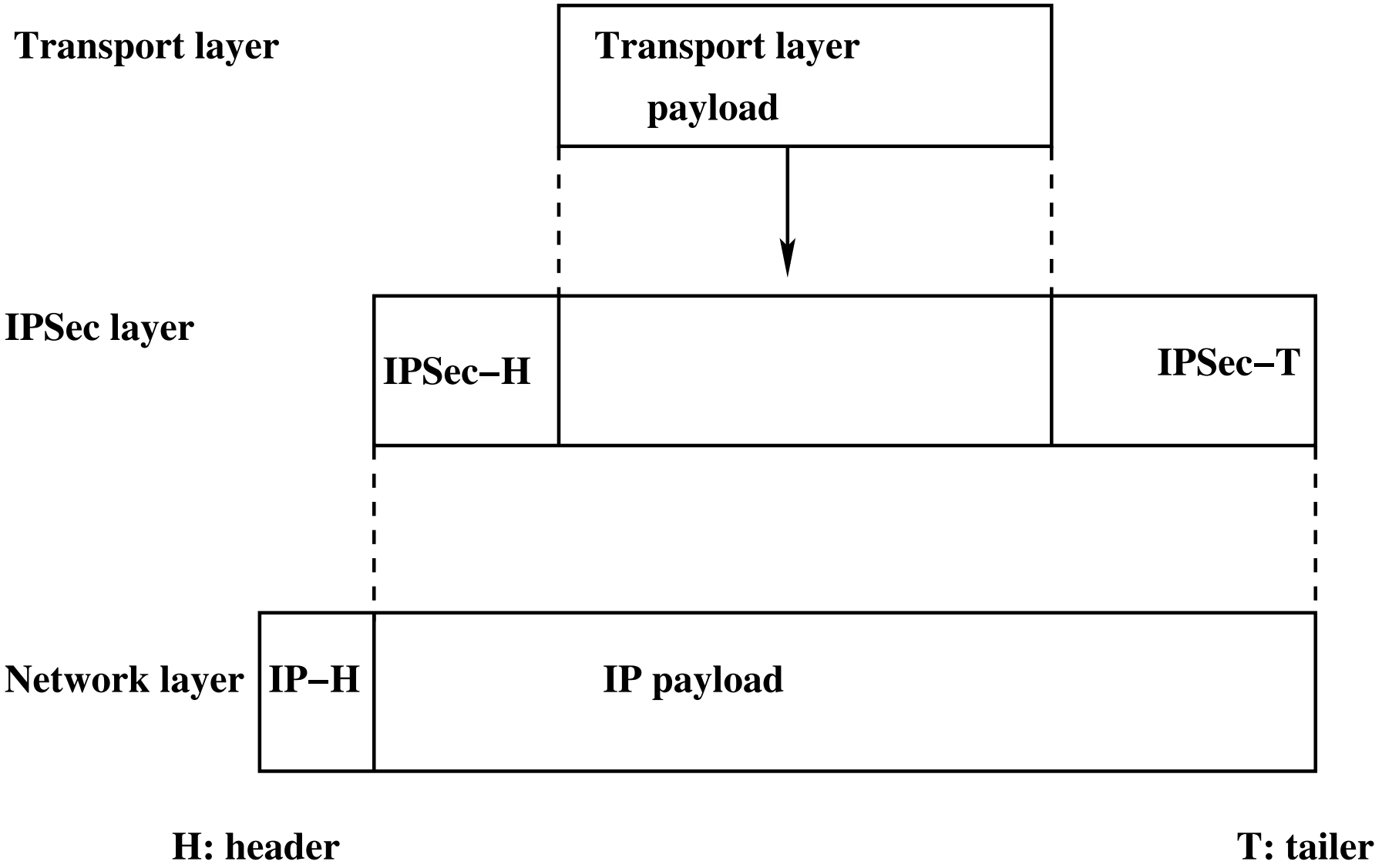
- IPSec is a collection of protocols designed by the Internet Engineering Task Force (IETF) to provide security for a packet at the network layer.
- IPSec helps create authenticated and credential packets for the IP layer.

Different Modes

Transport mode

- In this mode, IPSec protects what is delivered from the transport layer to the network layer.
- In other words, transport mode protects the network layer payload, the payload to be encapsulated in the network layer.
- Note that the transport mode does not protect the IP header.

IPSec in transport mode



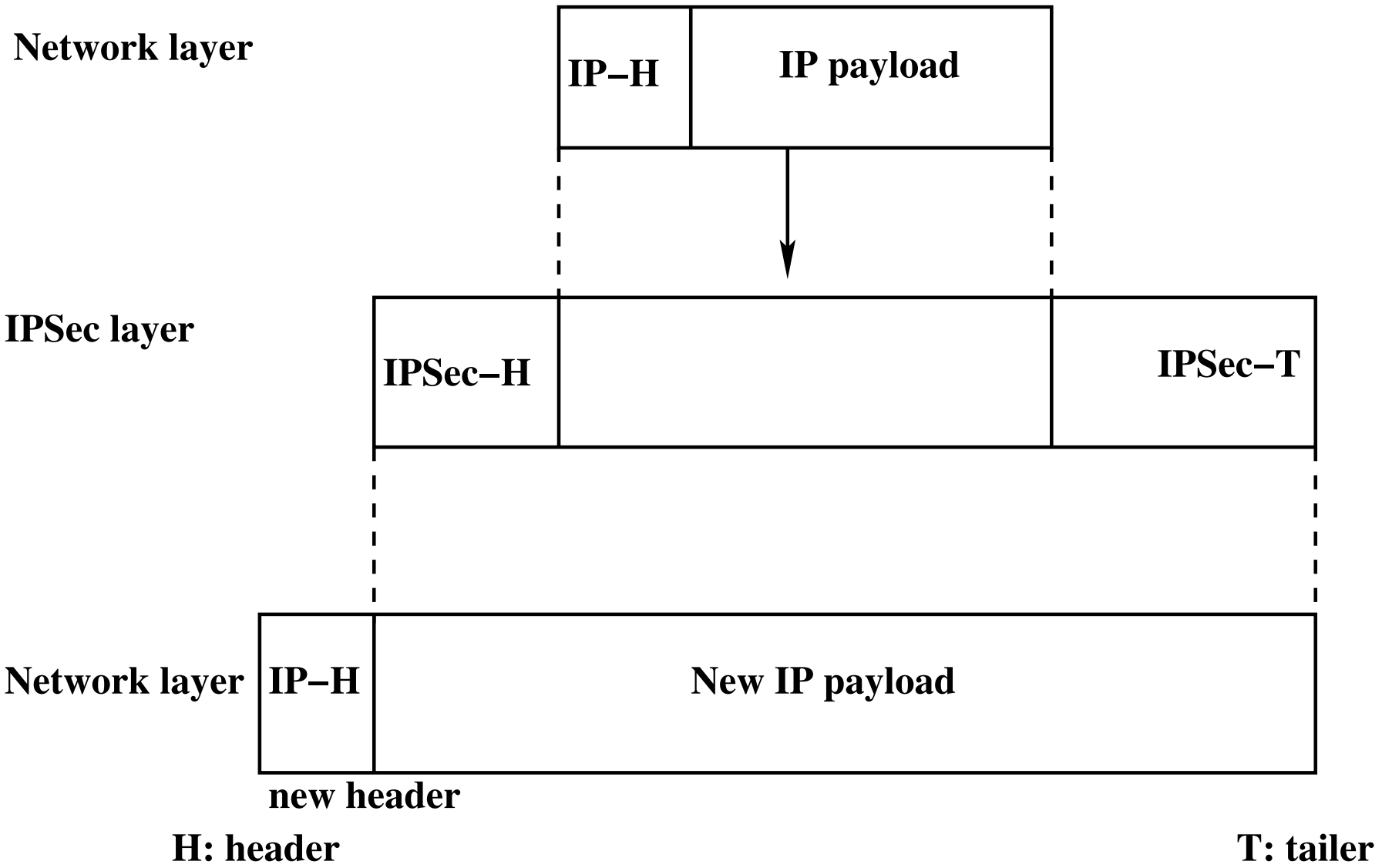
Transport mode

- This mode is normally used when we need host-to-host (end-to-end) protection of data.
- The sending host uses IPSec to authenticate and/or encrypt the payload delivered from the transport layer.
- The receiving host uses IPSec to check the authentication and/or decrypt the IP packet and deliver it to the transport layer.

Tunnel mode

- In this mode, IPSec protects the entire IP packet.
- It takes an IP packet, including the header, applies IPSec security methods to the entire packet, and then adds a new IP header.

IPSec in tunnel mode



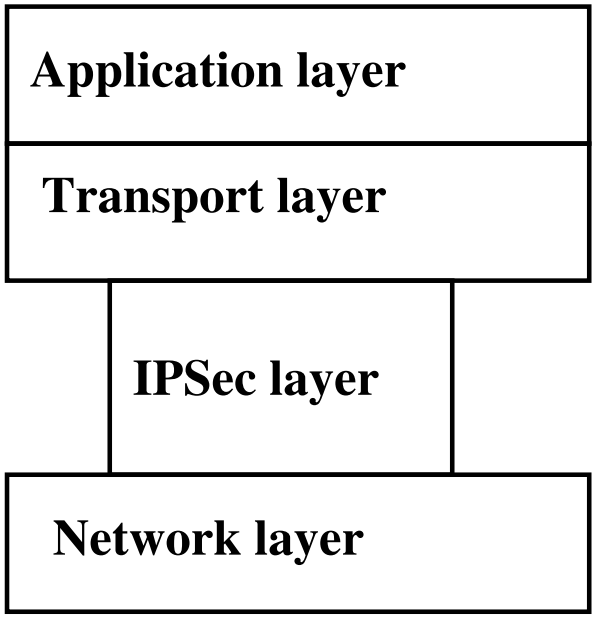
Tunnel mode

- The new IP header has different information than the original IP header.
- Tunnel mode is normally used between two routers, between a host and a router, or between a router and a host.
- In other words, tunnel mode is used when either the sender or the receiver is not a host.
- The entire original packet is protected from intrusion between the sender and the receiver, as if the whole packet goes through an imaginary tunnel.

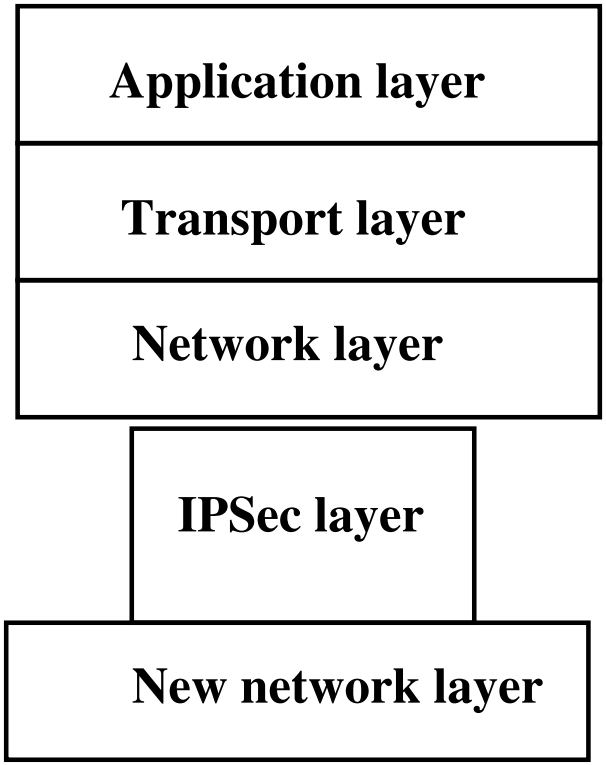
Transport mode *versus* Tunnel mode

- In transport mode, the IPSec layer comes between the transport layer and the network layer.
- In tunnel mode, the flow is from the network layer to the IPSec layer and then back to the network layer again.

Transport mode *versus* Tunnel mode



(a) Transport mode



(b) Tunnel mode

Layer-wise Network Security Protocols

Transport Layer

- Secure Socket Layer (SSL) provides security services between TCP and applications that use TCP. The Internet standard version is called Transport Layer Service (TLS).
- SSL/TLS provides confidentiality using symmetric encryption and message integrity using a message authentication code.
- SSL/TLS includes protocol mechanisms to enable two TCP users to deter- mine the security mechanisms and services they will use.
- HTTPS (HTTP over SSL) refers to the combination of HTTP and SSL to implement secure communication between a Web browser and a Web server.
- Secure Shell (SSH) provides secure remote logon and other secure client/server facilities.

Layer-wise Network Security Protocols

Application Layer

- **Pretty Good Privacy (PGP)**
  - PGP is an open-source, freely available software package for e-mail security. It provides authentication through the use of digital signature, confidentiality through the use of symmetric block encryption, compression using the ZIP algorithm, and e-mail compatibility using the radix-64 encoding scheme.
  - PGP incorporates tools for developing a public-key trust model and public-key certificate management.
- **Secure/Multipurpose Internet Mail Extension (S/MIME)**
  - S/MIME is a security enhancement to the MIME Internet e-mail format standard based on technology from RSA Data Security.
  - S/MIME is an Internet standard approach to e-mail security that incorporates the same functionality as PGP.

Layer-wise Network Security Protocols

Application Layer

- **Secure Electronic Transaction (SET)**
  - SET is an open encryption and security specification designed to protect credit card transactions on the Internet.
  - SET emerged from a call for security standards by MasterCard and Visa in February 1996.
  - A wide range of companies were involved in developing the initial specification, including IBM, Microsoft, Netscape, RSA, Terisa, and Verisign.
  - Beginning in 1996, there have been numerous tests of the concept, and by 1998 the first wave of SET-compliant products was available.

SET Transaction

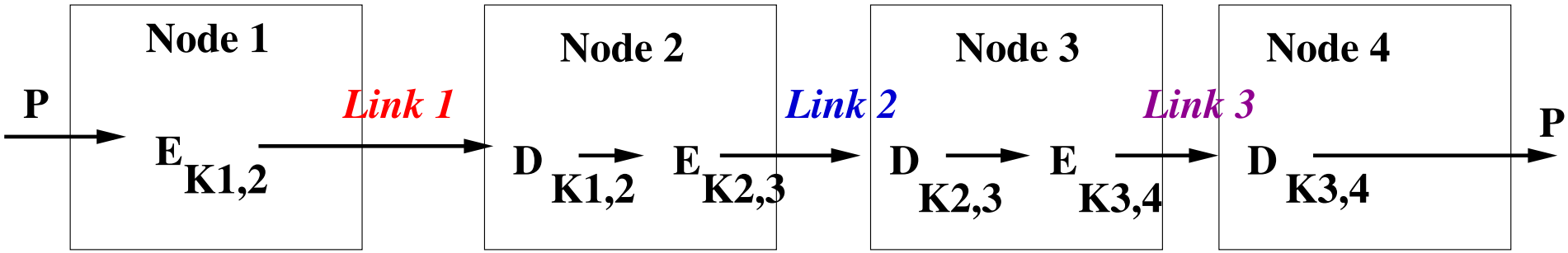
1. customer opens account
2. customer receives a certificate
3. merchants have their own certificates
4. customer places an order
5. merchant is verified
6. order and payment are sent
7. merchant requests payment authorization
8. merchant confirms order
9. merchant provides goods or service
10. merchant requests payment

Encrypting Communications Channels

Link-by-link encryption

- The easiest place to add encryption is at the physical layer.
- The interfaces to the physical layer are generally standardized, and it is easy to connect hardware encryption devices at this point.
- These devices encrypt all data passing through them, including data, routing information, and protocol information.
- They can be used on any type of digital communication link.
- On the other hand, any intelligent switching or storing nodes between the sender and the receiver need to decrypt the data stream before processing it.

Link-by-link encryption



P: plaintext message;
$K_{1,2}$: key shared between nodes 1 and 2;
$K_{2,3}$: key shared between nodes 2 and 3;
$K_{3,4}$: key shared between nodes 3 and 4;
$E_K(\cdot)$: encryption using the key K;
$D_K(\cdot)$: decryption using the key K.

Link-by-link encryption

Advantages

- Easier operation, since it can be made transparent to the user. That is, everything is encrypted before being sent over the link.
- Only one set of keys per link is required.
- Provides traffic-flow security, since any routing information is encrypted.

Link-by-link encryption

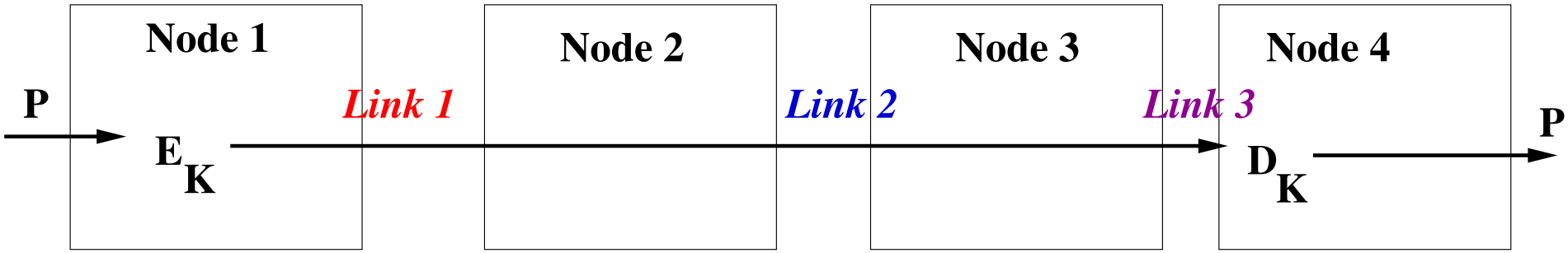
Disadvantages

- Data is exposed in the intermediate nodes.
- The biggest problem with encryption at the physical layer is that each physical link in the network needs to be encrypted: Leaving any link unencrypted reveals the security of the entire network.
  If the network is large, the cost may quickly become prohibitive for this kind of encryption.
- Additionally, every node in the network must be protected, since it processes unencrypted data.
  If all the network's users trust one another, and all nodes are in secure locations, this may be tolerable.

End-to-end encryption

- This approach is to put encryption equipment between the network layer and the transport layer.
- The encryption device must understand the data according to the protocols up to layer three and encrypt only the transport data units, which are then recombined with the un-encrypted routing information and sent to lower layers for transmission.
- This approach avoids the encryption/decryption problem at the physical layer.
- By providing EEE, the data remains encrypted until it reaches its final destination.

End-to-end encryption



P: plaintext message;
K: key shared between nodes 1 and 4;
$E_K(\cdot)$: encryption using the key K;
$D_K(\cdot)$: decryption using the key K.

End-to-end encryption

Advantages

- Higher secrecy level.

End-to-end encryption

Disadvantages

- The primary problem with EEE is that the routing information for the data is not encrypted; a good cryptanalyst can learn much from who is talking to whom, at what times and for how long, without ever knowing the contents of those conversations.
- Key management is also more difficult since individual users must make sure they have common keys.
- Traffic analysis is possible, since routing information is not encrypted.

Combining the Two: Link-by-link encryption and End-to-end encryption

- Combining the two, while most expensive, is the most effective way of securing a network.
- Encryption of each physical link makes any analysis of the routing information impossible, while end-to-end encryption reduces the threat of unencrypted data at the various nodes in the network.
- Key management for the two schemes can be completely separate:
  The network managers can take care of encryption at the physical level, while the individual users have responsibility for end-to-end encryption.

Comparing link-by-link encryption and end-to-end encryption

Link-by-link encryption	End-to-end encryption
Security within hosts	
1. Message exposed in sending host.	1. Message encrypted in sending host.
2. Message exposed in intermediate nodes.	2. Message remains encrypted in intermediate nodes.

Comparing link-by-link encryption and end-to-end encryption

Link-by-link encryption	End-to-end encryption
Role of user	
1. Applied by sending host.	1. Applied by sending process.
2. Invisible to user.	2. User applies encryption.
3. Host maintains encryption.	3. User must find algorithm.
4. One facility for all users.	4. User selects encryption.
5. Can be done in hardware.	5. More easily done in software.
6. All or no messages encrypted.	6. User chooses to encrypt or not, for each message.

Comparing link-by-link encryption and end-to-end encryption

Link-by-link encryption	End-to-end encryption
Implementation concerns	
1. Requires one key per host pair.	1. Requires one key per user pair.
2. Requires encryption hardware or software at each host.	2. Requires encryption hardware or software at each node.
3. Provides node authentication.	3. Provides user authentication.