Presentations

- EE295

Why read your paper?

- With support
  - What is the paper topic
  - The benefit of reading the paper
  - How will it change your life

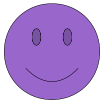
Hierarchy of understanding

- Images
- Diagrams
- Charts/graphs
- Text
- Tables

Simple rules to follow

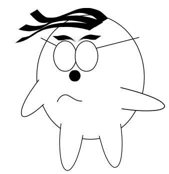
- 4 x 4 (four words, four lines)
- Phrases ★
  - Not speaker notes
- Single message per slide
- Builds to a conclusion

Make it readable

- Minimum 36 point font
- 50 point font
- Good contrast
  - Projectors have bad color
- Highlight important points 

Appearance

- Body language
  - Panic ?
  - Actions ?
- Dress
  - Casual professional



Tone and emotion

- Most positive == most important
- Finish strong and positive

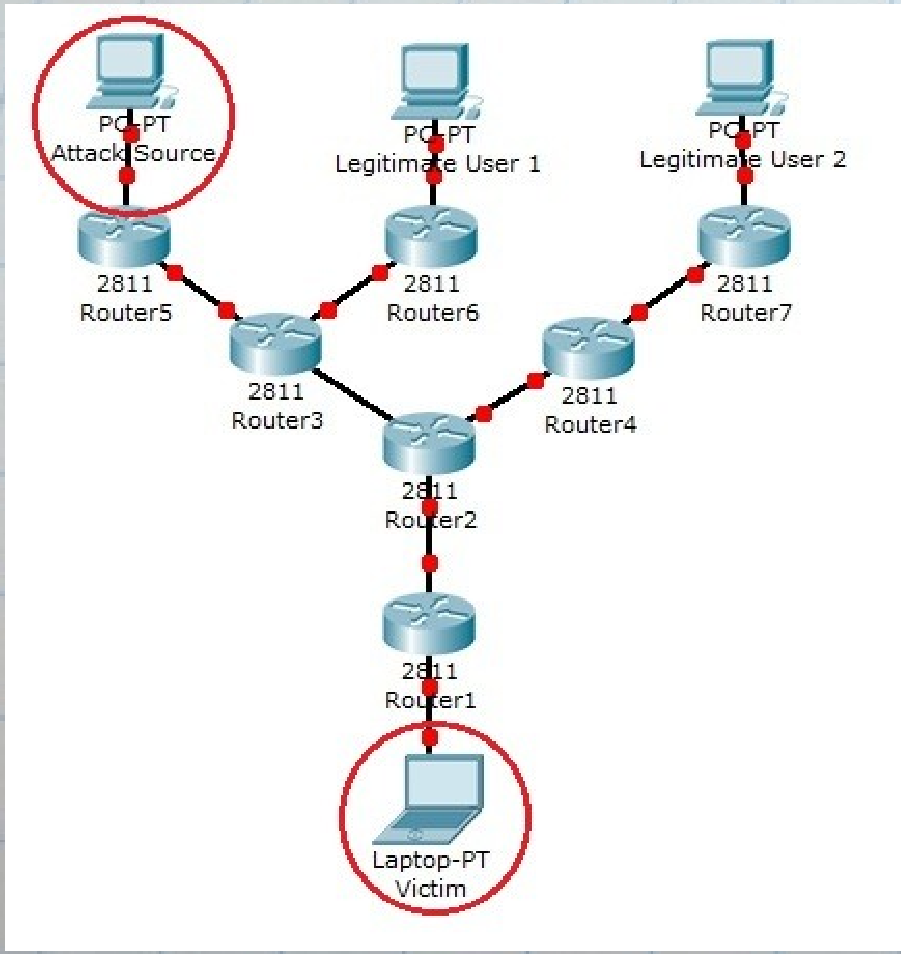
Rehearse

- Not natural
- Time factors
- Message factors
- Reduces panic

Slides from actual Presentations

Some Critical Review

DoS Attack



- ✓ Malicious attempt by an attacker to flood a network with packets.
- ✓ Overwhelm its data handling capacity such that the system becomes inaccessible.
- ✓ DoS attack is initiated by a single host.

Algorithms

```
For each packet 'p' from Source 'x' to Destination 'y':

if (logging entry not present)
        write address of router's interface through which the packet is going to be forwarded;
        set flag = 0;
else
        if (flag == 1)
                block the packet going through this router
        else
                do nothing
```

Logging Algorithm at Router

```
Receive the incoming packets;
if (rate of incoming packets goes beyond acceptable limit)
        send a blocking message with flag = 1 to the router from where the packet was received;
```

Traceback algorithm at the Victim computer

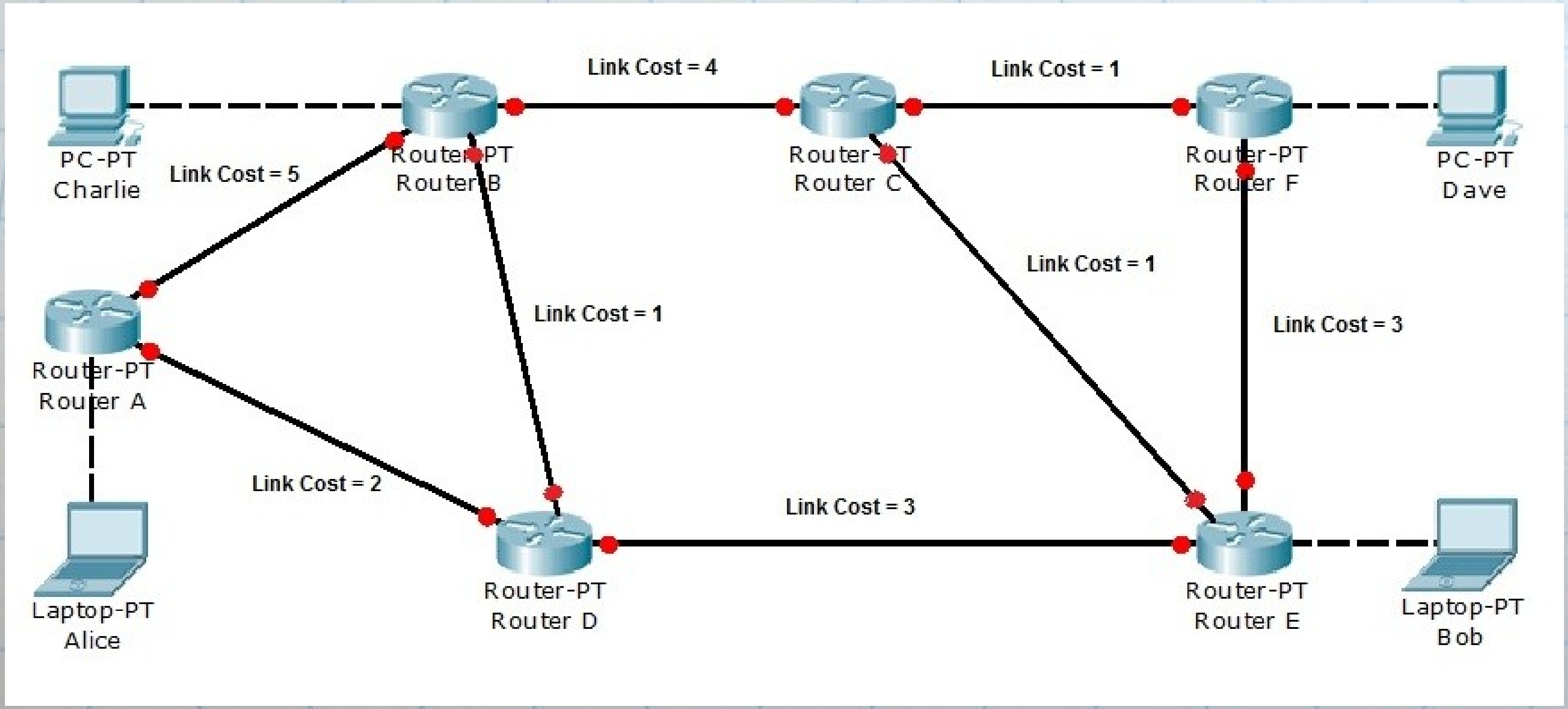
```
if ( message is a blocking message)
        for the specified route (source-destination), set flag bit = 1;
        forward the blocking message to the next router (referring to the log table for the address)
```

Traceback algorithm at the Router

Proposed IP Traceback Mechanism

- Efficiently traces the attack source without any false positives.
- Simpler, faster and effective way to tackle DoS attacks.
- Blocks all the routers along the attack path.
- Low overhead on routers as most the information used is already available with the routers.
- Only 33 bits of additional data is required to be logged into router.
- Allows tracing of multiple sources of attack.
- Low detection delay.

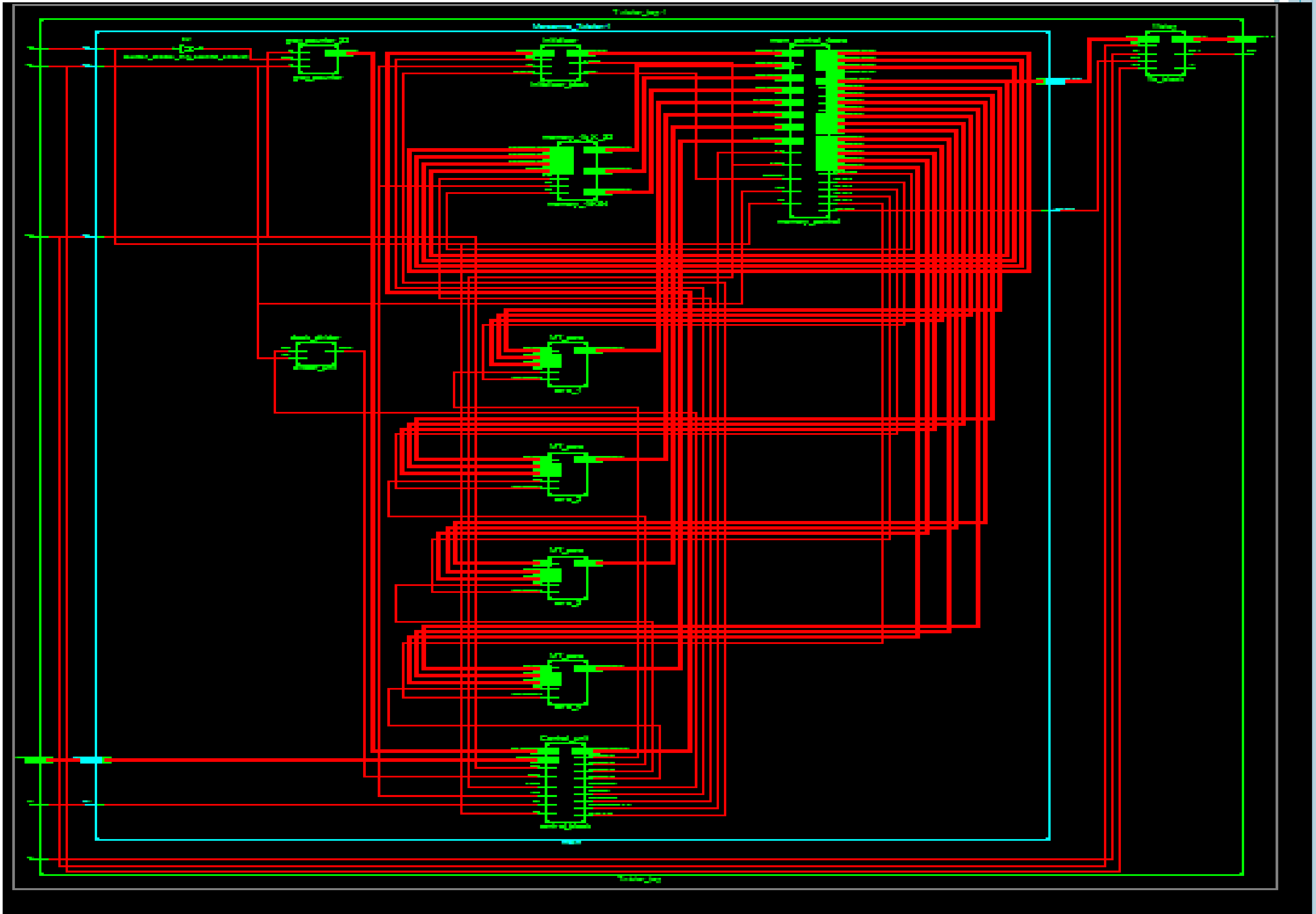
Attack Network



Randomness Results

Randomness Test	Measure	Ideal value	Software	Hardware
Chi-Square Test	Percentage	20% to 80%	72.44%	29.77%
Arithmetic mean	Mean value	127.500	127.5066	127.4789
Monte-carlo value of Pi	Pi value	3.141574059	3.141574059	3.141806341
Serial Correlation coefficient	Correlation coefficient	0.0 = uncorrelated	-0.000433	0.000304
Birthday Spacing test	p-value	[0,1]	0.083175	0.440985
The overlapping-5 permutation test	p-value	[0,1]	0.366844	0.852751
The Bit stream Test	p-value	[0,1]	0.58389	0.88988
OPSO, OQSO and DNA	p-value	[0,1]	0.3087	0.714
Parking lot test	p-value	[0,1]	0.620989	0.725731
Minimum distance test	p-value	[0,1]	0.003322	0.861518
The 3D Spheres test	p-value	[0,1]	0.622752	0.899760
The overlapping sums test	p-value	[0,1]	0.645970	0.322378
Runs test	p-value	[0,1]	0.550942	0.499031
Craps Test	p-value	[0,1]	0.386168	0.630164

RTL Schematic



```
  /**
   * The Packet that is currently being transmitted on the channel (or last
   * packet to have been transmitted on the channel if the channel is
   * free.)
   */
  Ptr<Packet> m_currentPkt;

  /**
   * Device Id of the source that is currently transmitting on the
   * channel. Or last source to have transmitted a packet on the
   * channel, if the channel is currently not busy.
   */
  uint32_t                  m_currentSrc;

  /**
   * Current state of the channel
   */
  WireState       m_state;
  bool              m_collision;
};

} // namespace ns3

namespace ns3 {

class Queue;
class RsmaChannel;
class ErrorModel;

/**
 * \defgroup csma RsmaNetDevice
 *
 * This section documents the API of the ns-3 csma module. For a generic functional description, please refer to the ns-3 manual.
 */

/**
 * \ingroup csma
 * \class RsmaNetDevice
 * \brief A Device for a Csma Network Link.
 *
 * The Csma net device class is analogous to layer 1 and 2 of the
 * TCP stack. The NetDevice takes a raw packet of bytes and creates a
 * protocol specific packet from them.
 */
class RsmaNetDevice : public NetDevice
```

Comparison with other Diversities.

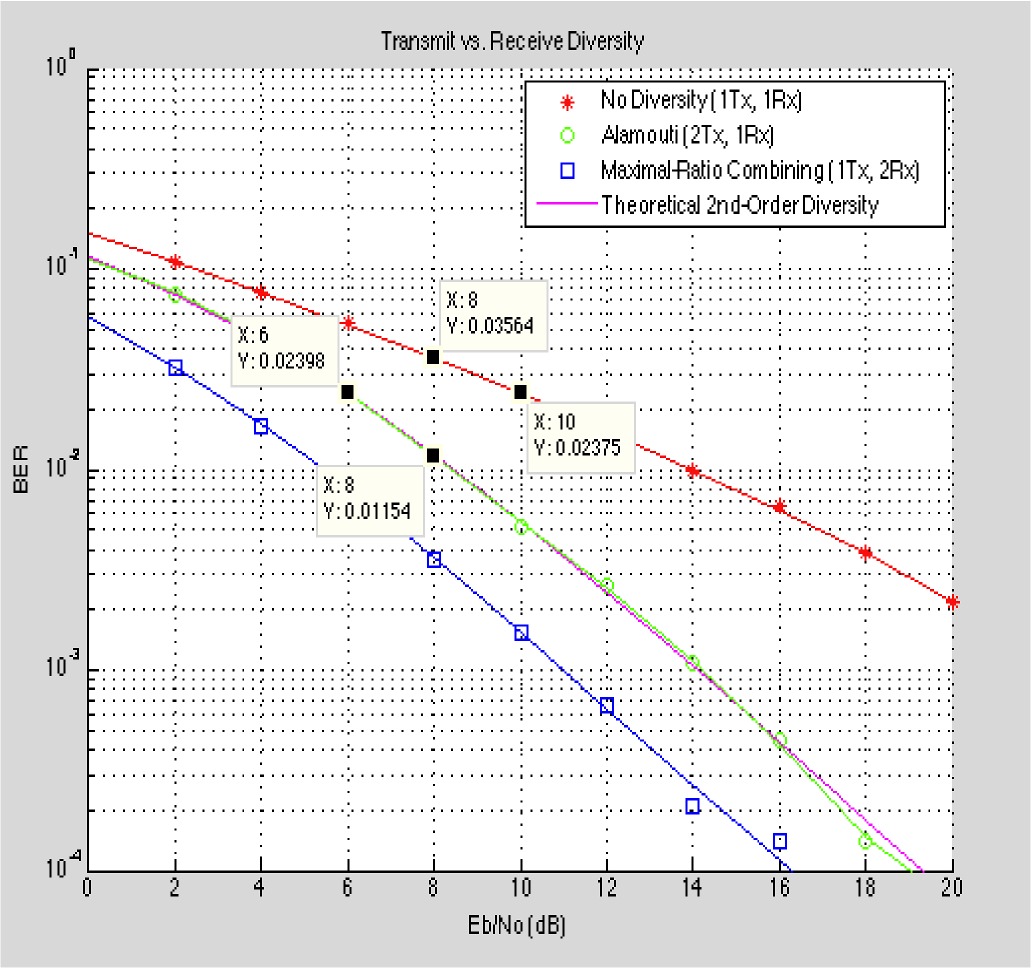


Figure 6[4]

- No Diversity Slop of BER curve is -1.
- Maximal Ratio diversity BER curve slope -2.
- Alamouti's Diversity curve BER slope of -2 but at a loss of 3dB.

Slides from prior proposal presentations

Overview of current protocols

1) HTTP - Header size of Hyper Text Transfer Protocol (HTTP) is 400 Bytes to 8KB[3]. Fig[4]
2) Continuous transmission of HTTP messages

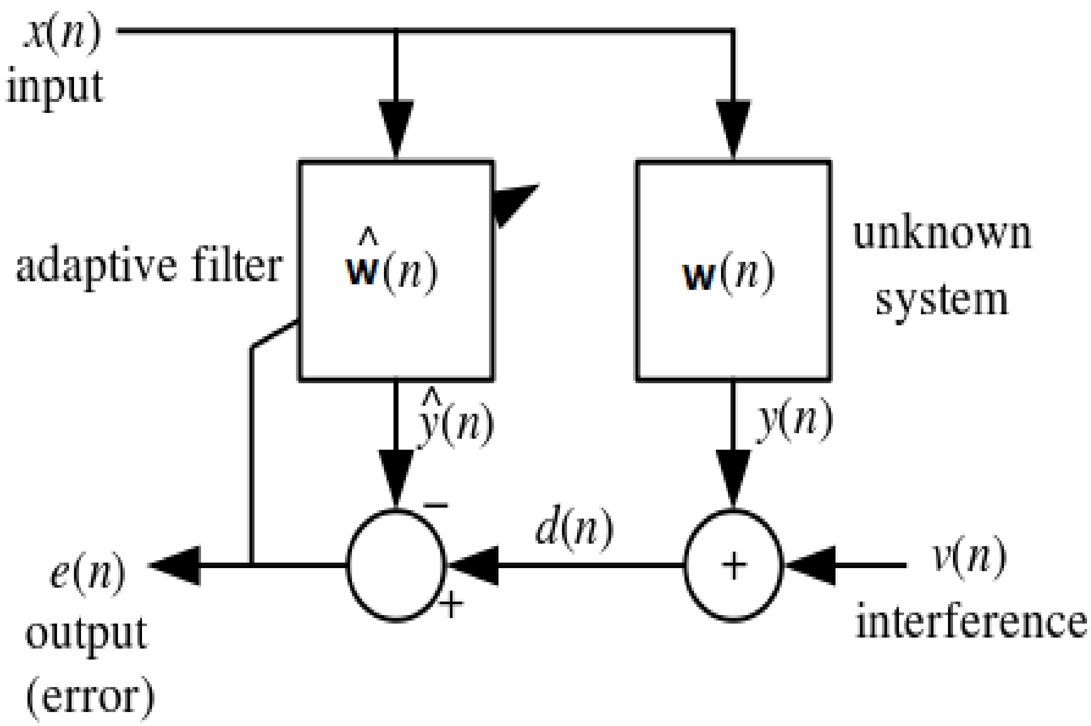
Example 2: HTTP request header

```
GET /PollingStock//PollingStock HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.5)
Gecko/20091102 Firefox/3.5.5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.example.com/PollingStock/
Cookie: showInheritedConstant=false;
showInheritedProtectedConstant=false; showInheritedProperty=false;
showInheritedProtectedProperty=false; showInheritedMethod=false;
showInheritedProtectedMethod=false; showInheritedEvent=false;
showInheritedStyle=false; showInheritedEffect=false
```

Example 3: HTTP response header

```
HTTP/1.x 200 OK
X-Powered-By: Servlet/2.5
Server: Sun Java System Application Server 9.1_02
Content-Type: text/html;charset=UTF-8
Content-Length: 21
Date: Sat, 07 Nov 2009 00:32:46 GMT
```

Mathematics



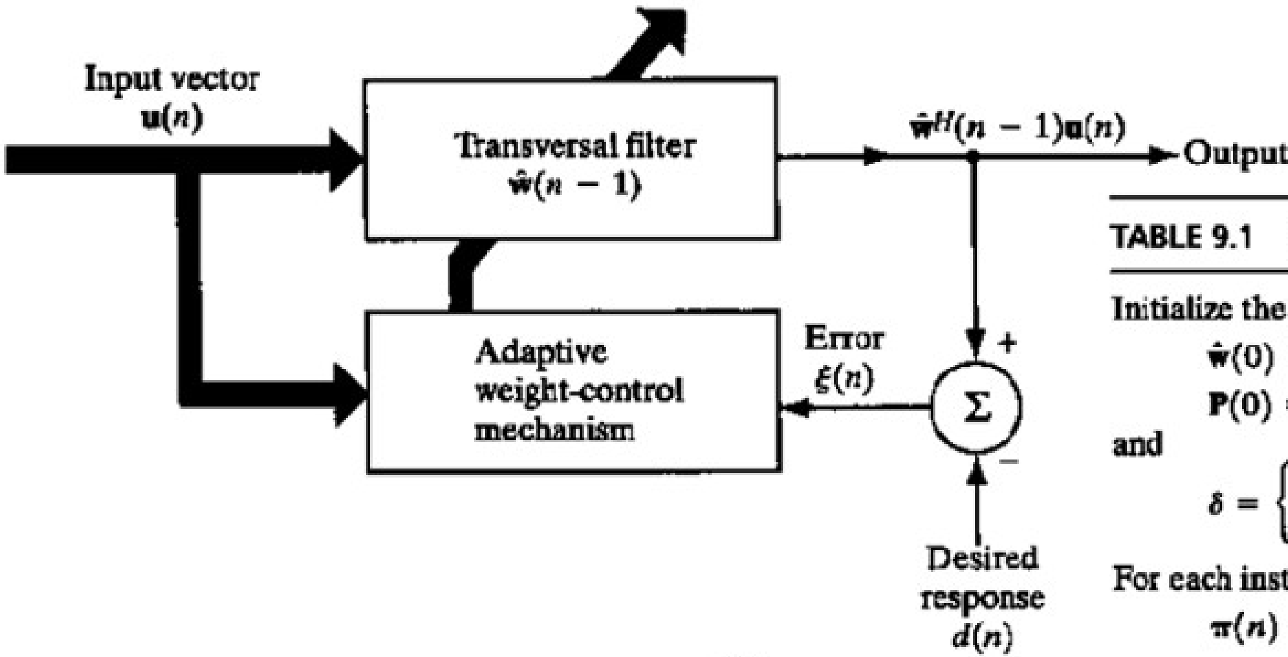
$$y(n) = \sum_{i=0}^{N-1} w(n)x(n-i) = \mathbf{w}^T(n)\mathbf{x}(n)$$

$$e(n)=d(n)-y(n)$$

$$\mu(n) = \frac{1}{\mathbf{x}^T(n)\mathbf{x}(n)}$$

$$\mathbf{w}(n+1) = \mathbf{w}(n) + \mu(n)e(n)\mathbf{x}(n)$$

RLS Noise Cancellation Circuit



(a)

TABLE 9.1 Summary of the RLS Algorithm

Initialize the algorithm by setting

$$\hat{\mathbf{w}}(0) = \mathbf{0},$$

$$\mathbf{P}(0) = \delta^{-1}\mathbf{I},$$

and

$$\delta = \begin{cases} \text{small positive constant for high SNR} \\ \text{large positive constant for low SNR} \end{cases}$$

For each instant of time, $n = 1, 2, \ldots,$ compute

$$\boldsymbol{\pi}(n) = \mathbf{P}(n-1)\mathbf{u}(n),$$

$$\mathbf{k}(n) = \frac{\boldsymbol{\pi}(n)}{\lambda + \mathbf{u}^H(n)\boldsymbol{\pi}(n)},$$

$$\xi(n) = d(n) - \hat{\mathbf{w}}^H(n-1)\mathbf{u}(n),$$

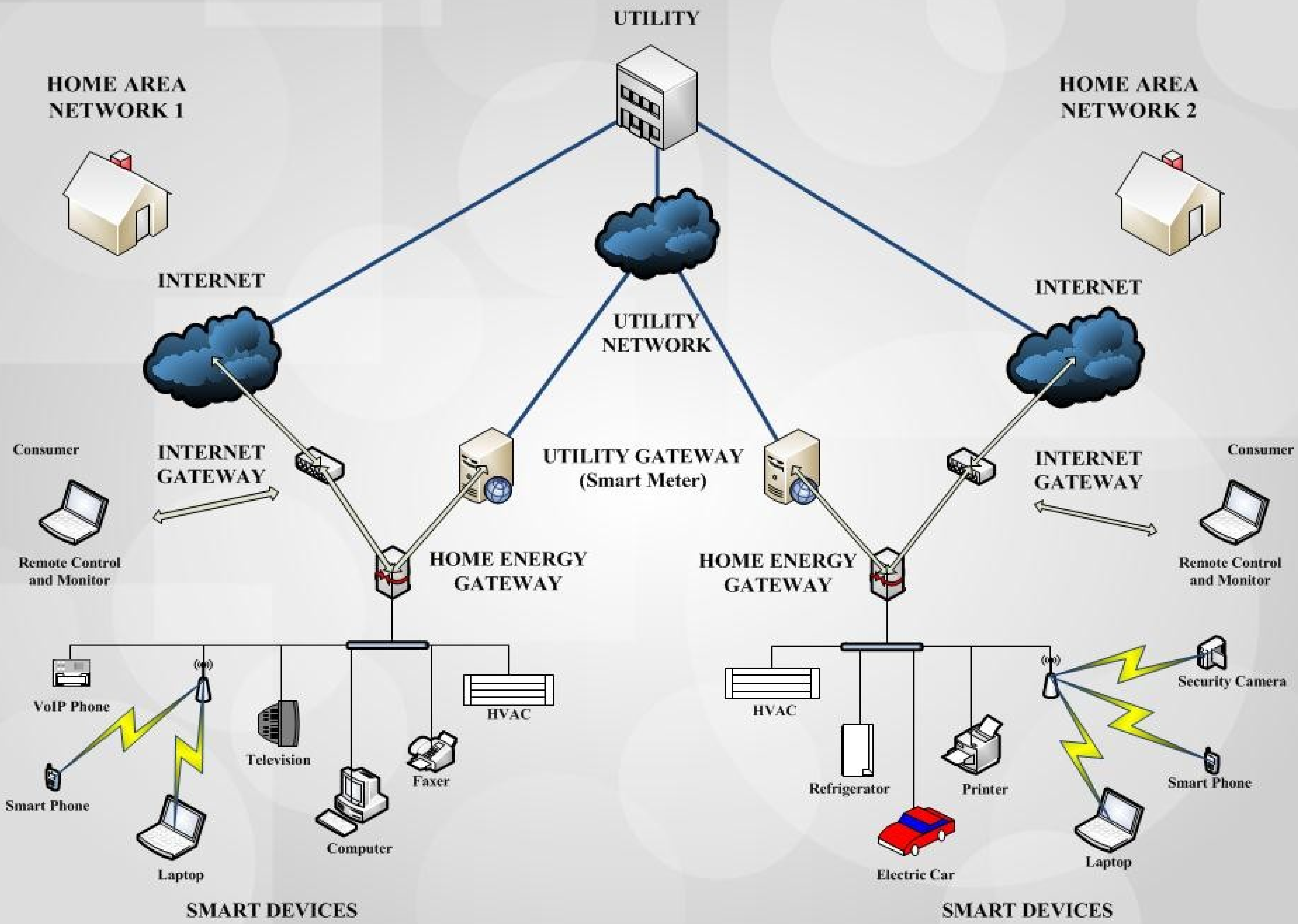
$$\hat{\mathbf{w}}(n) = \hat{\mathbf{w}}(n-1) + \mathbf{k}(n)\xi^*(n),$$

and

$$\mathbf{P}(n) = \lambda^{-1}\mathbf{P}(n-1) - \lambda^{-1}\mathbf{k}(n)\mathbf{u}^H(n)\mathbf{P}(n-1).$$

Traditional Method - Low pass Filters

- In image or video processing, one of the most prominent problems is degradation by noise and to overcome this issue, the images are passed through a low pass filter that helps reduce visible noise.
- Traditionally all the Low Pass filter uses the principle of Averaging the neighborhood of pixels and applying this averaged value as input.
- The problem occurs when large numbers of iterations are performed and **edges regions** are also included in the averaging process.
- This results in degradation of quality of image and makes it look very blurred.


UTILITY
HOME AREA NETWORK 1
HOME AREA NETWORK 2
INTERNET
UTILITY NETWORK
INTERNET
Consumer
INTERNET GATEWAY
UTILITY GATEWAY (Smart Meter)
INTERNET GATEWAY
Consumer
Remote Control and Monitor
HOME ENERGY GATEWAY
HOME ENERGY GATEWAY
Remote Control and Monitor
VoIP Phone
HVAC
HVAC
Security Camera
Television
Smart Phone
Faxer
Refrigerator
Printer
Smart Phone
Computer
Laptop
Electric Car
Laptop
SMART DEVICES
SMART DEVICES

SCALABILITY ON A LOAD BALANCER

- Achieved in applications by creating a server cluster or a server farm.
- These are collections of servers that distribute the workload amongst themselves
- The solution is designed to make adding more servers easy and efficient in order to handle increasing workloads
- This is far more preferable to adding more resources to a single server for reasons of cost, reliability and efficiency