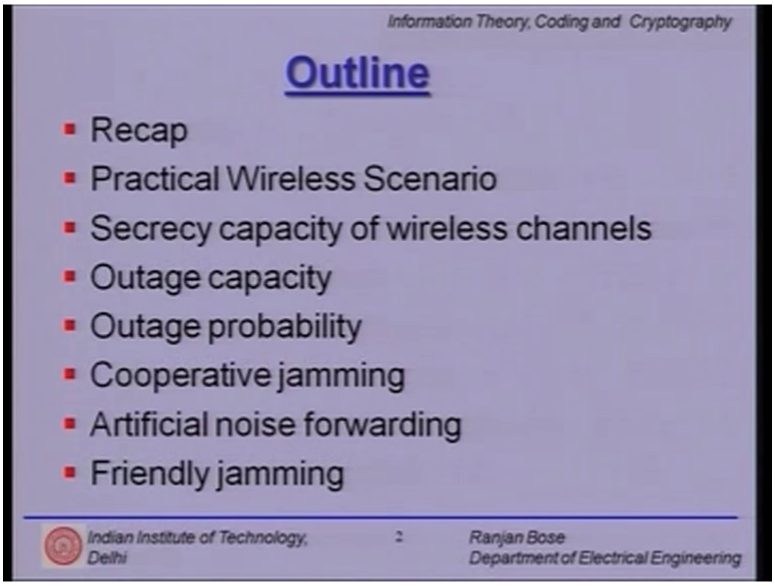
Information Theory, Coding and Cryptography
Dr. Ranjan Bose
Department of Electrical Engineering
Indian Institute of Technology, Delhi

Module - 39
Physical Layer Security
Lecture - 39

Hello and welcome to our module on Physical Layer Security. Let us start with a brief outline for today's talk.

(Refer Slide Time: 00:34)



Information Theory, Coding and Cryptography

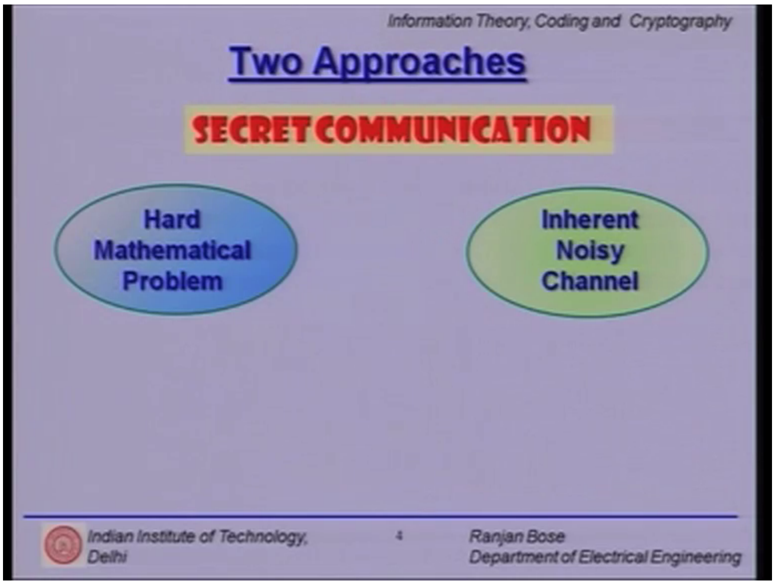
Outline

- Recap
- Practical Wireless Scenario
- Secrecy capacity of wireless channels
- Outage capacity
- Outage probability
- Cooperative jamming
- Artificial noise forwarding
- Friendly jamming

Indian Institute of Technology, Delhi 2 Ranjan Bose Department of Electrical Engineering

We will start with a brief recap: we will talk about practical wireless scenario in the context of physical layer security. We will then talk about secrecy capacity of wireless channels, we will define outage capacity; talk about outage probability and then look at some practical's schemes like cooperative jamming, artificial noise forwarding and friendly jamming.

(Refer Slide Time: 01:04)



Information Theory, Coding and Cryptography

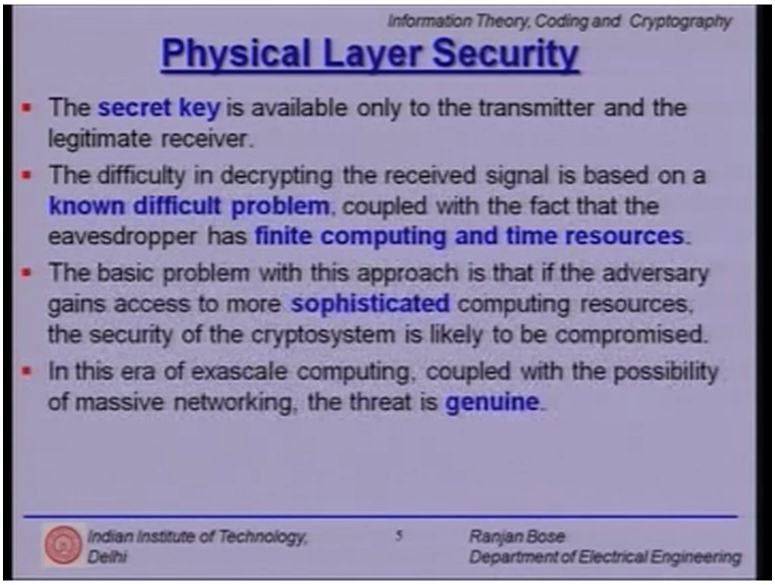
Two Approaches

SECRET COMMUNICATION

Indian Institute of Technology, Delhi 4 Ranjan Bose Department of Electrical Engineering

So, let us start with the basic idea about secret communications. As we have observed earlier there are two ways to do secret communications. Either have hard mathematical problem to solve which the eavesdropper or the adversary will take time and computing resources to solve or use the inherent noisy nature of the channel and provide security at the physical layer. This lecture concerns with second approach how to use the inherent noisy nature of the channel and provide information theoretic security.

(Refer Slide Time: 01:43)



Information Theory, Coding and Cryptography

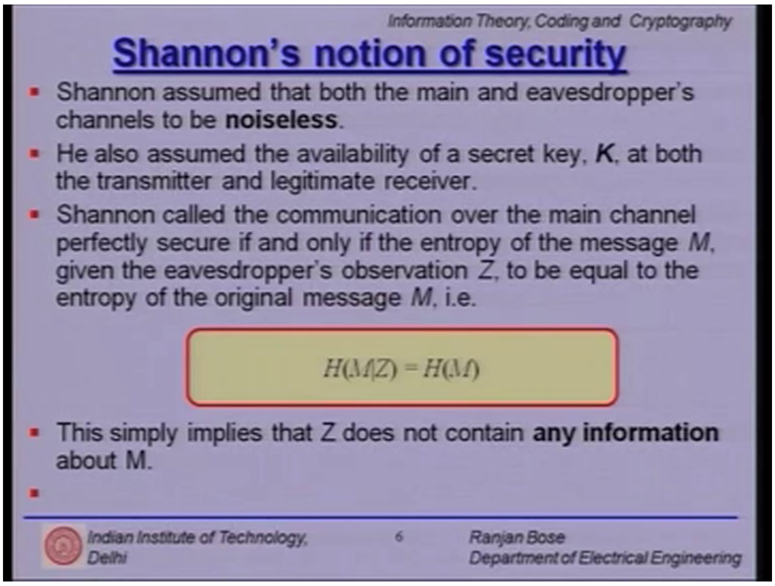
Physical Layer Security

- The **secret key** is available only to the transmitter and the legitimate receiver.
- The difficulty in decrypting the received signal is based on a **known difficult problem**, coupled with the fact that the eavesdropper has **finite computing and time resources**.
- The basic problem with this approach is that if the adversary gains access to more **sophisticated** computing resources, the security of the cryptosystem is likely to be compromised.
- In this era of exascale computing, coupled with the possibility of massive networking, the threat is **genuine**.

Indian Institute of Technology, Delhi 5 Ranjan Bose Department of Electrical Engineering

So, quick recap what we have assumed so far is that secret key is available only to the transmitter and receiver and the secrecy in classical cryptography is based on solving known difficult problem using finite computing and time resources. But we have also observed that computing systems are becoming more and more sophisticated networked distributed and the threat is genuine.

(Refer Slide Time: 02:14)



Information Theory, Coding and Cryptography

Shannon's notion of security

- Shannon assumed that both the main and eavesdropper's channels to be **noiseless**.
- He also assumed the availability of a secret key, ***K***, at both the transmitter and legitimate receiver.
- Shannon called the communication over the main channel perfectly secure if and only if the entropy of the message *M*, given the eavesdropper's observation *Z*, to be equal to the entropy of the original message *M*, i.e.

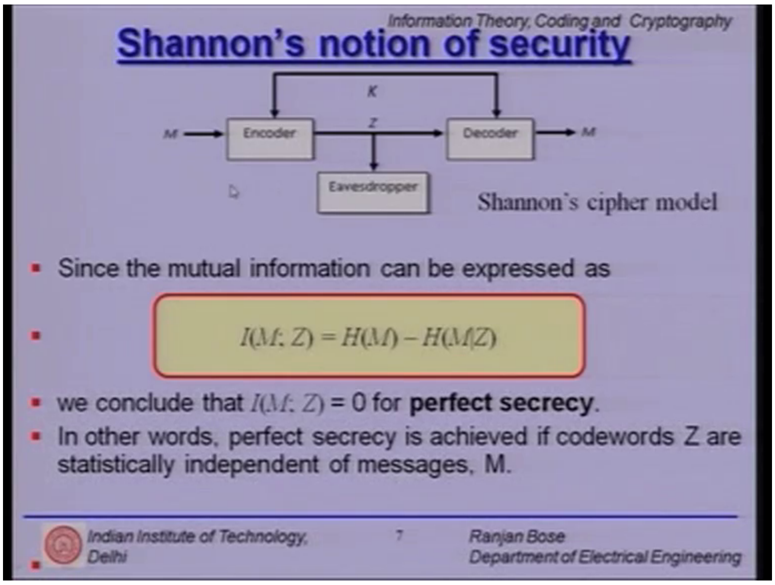
$$H(M|Z) = H(M)$$

- This simply implies that Z does not contain **any information** about M.
-

Indian Institute of Technology, Delhi 6 Ranjan Bose Department of Electrical Engineering

In the last lecture we have talked about Shannon's notion of security. The Shannon assumed that both the main channel and eavesdroppers channel was noise less. However, they had the same shared key K which was used to encode and decode the message. And what channel said is therefore perfect secrecy H of M given Z entropy of the message M given the observation of the eavesdroppers Z is nothing but H of M; that is no information is conveyed via Z, Z has not contain any information about M.

(Refer Slide Time: 02:52)



Information Theory, Coding and Cryptography

Shannon's notion of security

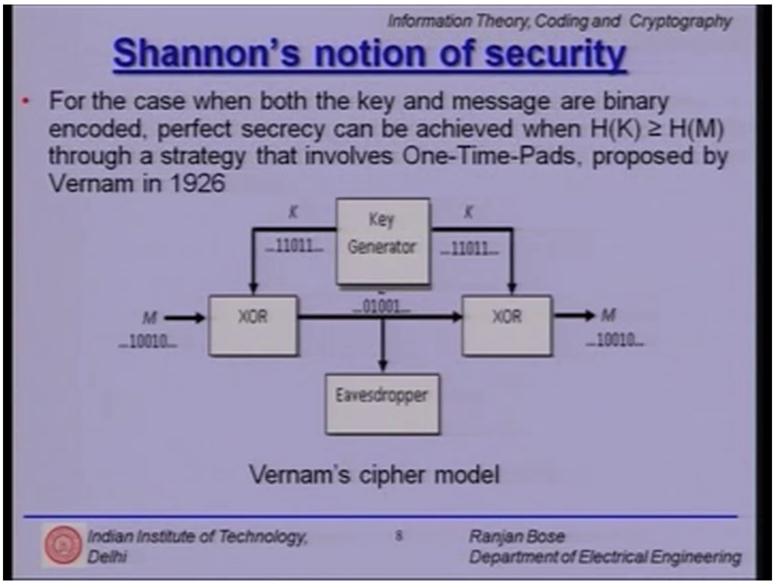
Shannon's cipher model

- Since the mutual information can be expressed as
- $$I(M; Z) = H(M) - H(M|Z)$$
- we conclude that $I(M; Z) = 0$ for **perfect secrecy**.
- In other words, perfect secrecy is achieved if codewords Z are statistically independent of messages, M.

Indian Institute of Technology, Delhi 7 Ranjan Bose Department of Electrical Engineering

So, the block diagram looks like this M message goes to the encoder using the key K is encoded in to Z which is decoded using the decoder using the same key K and gives back M, no noise anywhere in the channel. So, eavesdropper has his hands on Z and his job is to find out M from Z. So, I of M semicolon Z the mutual information between the message and the observation of eavesdropper is nothing but H of M minus H of M given Z. And what Shannon suggested is that H the sorry the I M semicolon Z should be equal to 0 for perfect secrecy. What it means is perfect secrecy is achieved if codeword Z and message M are statistically independent.

(Refer Slide Time: 03:48)



Information Theory, Coding and Cryptography

Shannon's notion of security

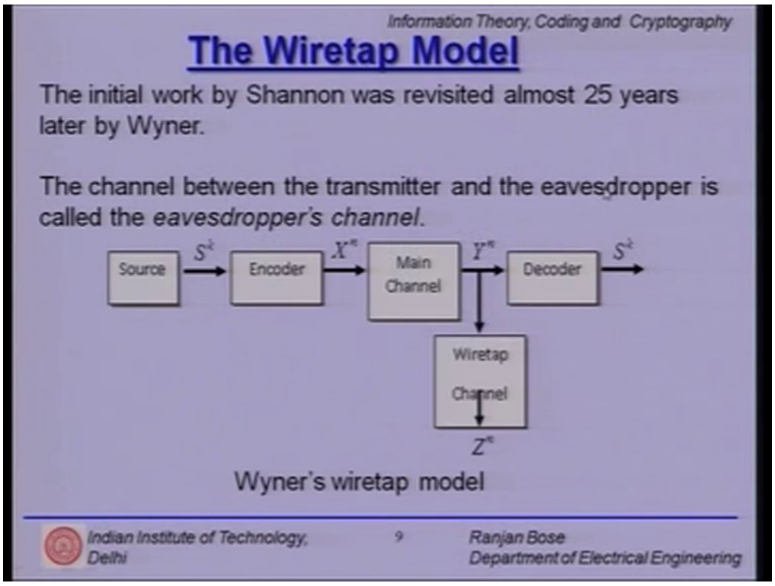
- For the case when both the key and message are binary encoded, perfect secrecy can be achieved when H(K) ≥ H(M) through a strategy that involves One-Time-Pads, proposed by Vernam in 1926

Vernam's cipher model

Indian Institute of Technology, Delhi 8 Ranjan Bose Department of Electrical Engineering

Now, for the case when both the key and the message of binary we have the message M we use XOR function, we get another binary stream it is XORed back with the key K and we get the message and eavesdropper uses this binary version. And what Shannon had shown is for perfect secrecy we should have H of K the key should be greater than or equal to H of M the message, that is the key should be at least as big as the message and this was achieved using One-Time-Pads proposed by Vernam.

(Refer Slide Time: 04:27)



Information Theory, Coding and Cryptography

The Wiretap Model

The initial work by Shannon was revisited almost 25 years later by Wyner.

The channel between the transmitter and the eavesdropper is called the *eavesdropper's channel*.

Source $\xrightarrow{S^k}$ Encoder $\xrightarrow{X^n}$ Main Channel $\xrightarrow{Y^n}$ Decoder $\xrightarrow{\hat{S}^k}$

Wiretap Channel $\rightarrow Z^n$

Wyner's wiretap model

Indian Institute of Technology, Delhi

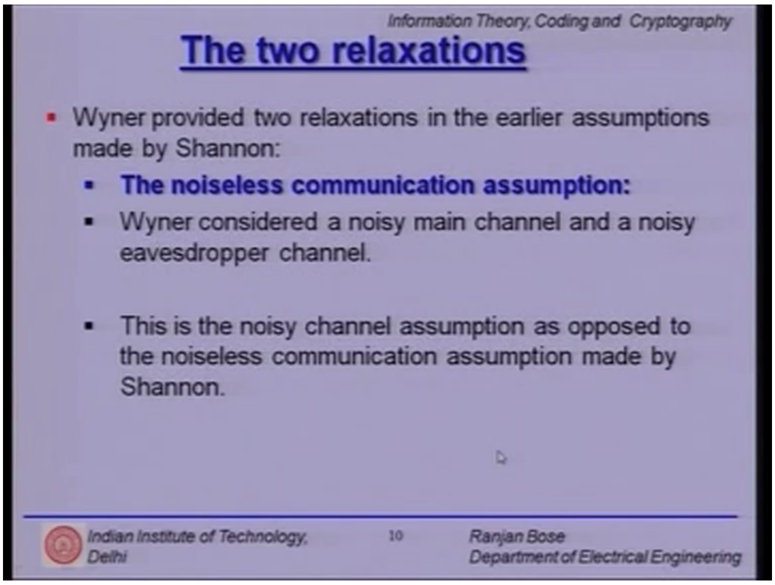
9

Ranjan Bose
Department of Electrical Engineering

We had also looked at the wiretap modeled which was initiated by Wyner almost 25 years later and here we have the source, it goes to an encoder which generate X of n. So, n is the block length of the code which is sent over the main channel, but this main channel is noisy that is the first assumption made by Wyner and what we get is Y n which is decoded back.

Now, this may or may not be always correct because there is a finite probability of error. On the other hand there is a wiretap which is also noisy and the eavesdropper gets Z n.

(Refer Slide Time: 05:09)



Information Theory, Coding and Cryptography

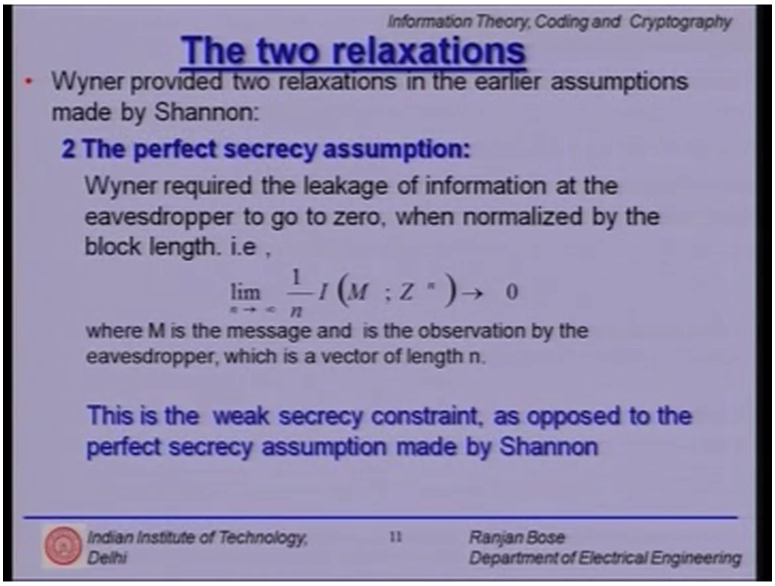
The two relaxations

- Wyner provided two relaxations in the earlier assumptions made by Shannon:
  - **The noiseless communication assumption:**
  - Wyner considered a noisy main channel and a noisy eavesdropper channel.
  - This is the noisy channel assumption as opposed to the noiseless communication assumption made by Shannon.

Indian Institute of Technology, Delhi 10 Ranjan Bose Department of Electrical Engineering

So, the two relaxations made by Wyner are the noiseless communication assumption, where Wyner assume that the noisy main channel and noisy eavesdropper channel is present in the system.

(Refer Slide Time: 05:24)



Information Theory, Coding and Cryptography

The two relaxations

- Wyner provided two relaxations in the earlier assumptions made by Shannon:

2 The perfect secrecy assumption:

Wyner required the leakage of information at the eavesdropper to go to zero, when normalized by the block length. i.e ,

$$\lim_{n \to \infty} \frac{1}{n} I\left(M \; ; Z^{n}\right) \to \quad 0$$

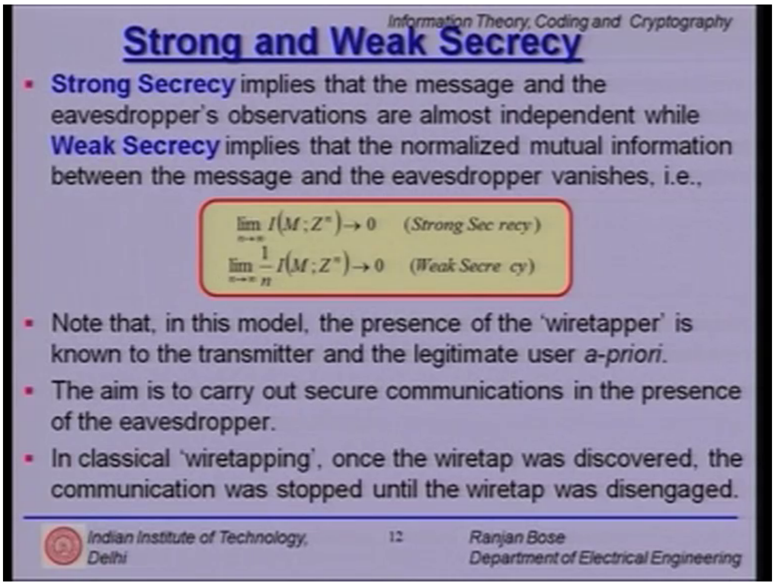
where M is the message and is the observation by the eavesdropper, which is a vector of length n.

This is the weak secrecy constraint, as opposed to the perfect secrecy assumption made by Shannon

Indian Institute of Technology, Delhi 11 Ranjan Bose Department of Electrical Engineering

The second assumption is the relaxation of the perfect secrecy condition wherein he said that the normalized leakage of information I M semicolon Z n normalized by the block length n should tend to 0 as limit n tends to 0; n here is the block length, M is the message, Z n is the observation of the eavesdrop. This is the week secrecy constrained as opposed to the perfect secrecy assumptions made by Shannon.

(Refer Slide Time: 05:51)



Information Theory, Coding and Cryptography

Strong and Weak Secrecy

- **Strong Secrecy** implies that the message and the eavesdropper's observations are almost independent while **Weak Secrecy** implies that the normalized mutual information between the message and the eavesdropper vanishes, i.e.,

$$\lim_{n\to\infty} I(M;Z^n) \to 0 \quad (\textit{Strong Sec recy})$$

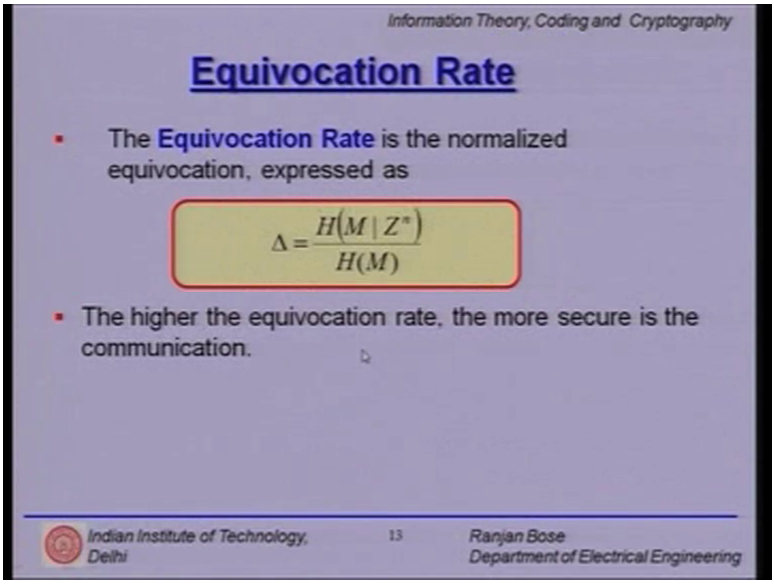
$$\lim_{n\to\infty} \frac{1}{n} I(M;Z^n) \to 0 \quad (\textit{Weak Secre cy})$$

- Note that, in this model, the presence of the 'wiretapper' is known to the transmitter and the legitimate user *a-priori*.
- The aim is to carry out secure communications in the presence of the eavesdropper.
- In classical 'wiretapping', once the wiretap was discovered, the communication was stopped until the wiretap was disengaged.

Indian Institute of Technology, Delhi 12 Ranjan Bose Department of Electrical Engineering

Then we had looked at strong and weak secrecy and the strong secrecy condition we had observed is the mutual information between the message and the observation of the eavesdropper tends to 0, as n tends to infinity. And the normalized mutual information 1 over n I M semicolon Z n tends to 0 as the weak secrecy condition as n tends to infinity.

(Refer Slide Time: 06:20)



Information Theory, Coding and Cryptography

Equivocation Rate

- The **Equivocation Rate** is the normalized equivocation, expressed as

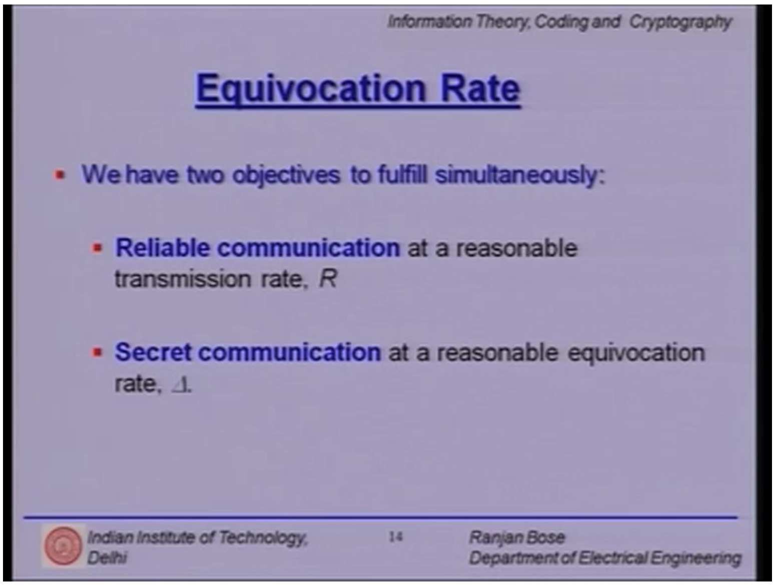
$$\Delta = \frac{H(M \mid Z^n)}{H(M)}$$

- The higher the equivocation rate, the more secure is the communication.

Indian Institute of Technology, Delhi 13 Ranjan Bose Department of Electrical Engineering

It also defined equivocation rate as normalized H M given Z n normalized by the factor H of M, the entropy of the message.

(Refer Slide Time: 06:33)



Information Theory, Coding and Cryptography

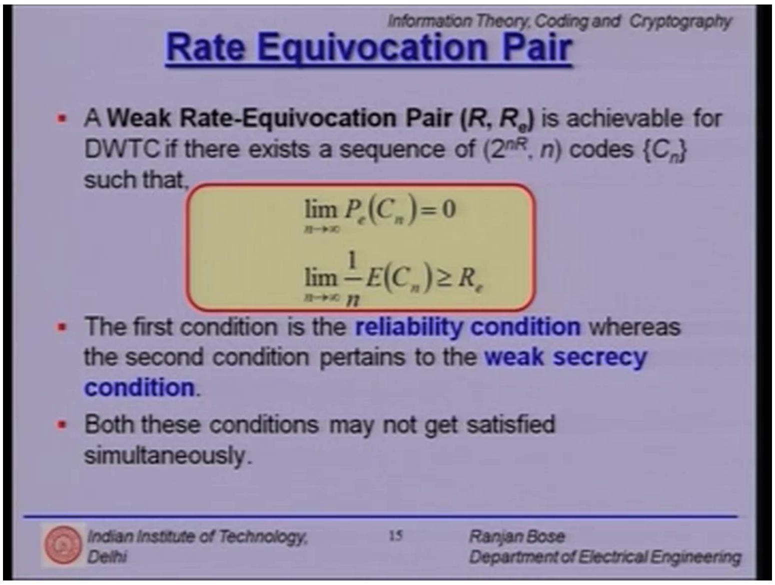
Equivocation Rate

- We have two objectives to fulfill simultaneously:
  - **Reliable communication** at a reasonable transmission rate, R
  - **Secret communication** at a reasonable equivocation rate, Δ.

Indian Institute of Technology, Delhi 14 Ranjan Bose Department of Electrical Engineering

We have to also look at the two objectives to be satisfied. One is that of reliable communication. So, at a reasonable transmission rate we should have probability of error tending to 0 and then we have the requirement for secret communication at a reasonable equivocation rate delta.

(Refer Slide Time: 06:55)



Information Theory, Coding and Cryptography

Rate Equivocation Pair

- A **Weak Rate-Equivocation Pair (R, R_e)** is achievable for DWTC if there exists a sequence of (2^{nR}, n) codes $\{C_n\}$ such that,

$$\lim_{n\to\infty} P_e(C_n)=0$$

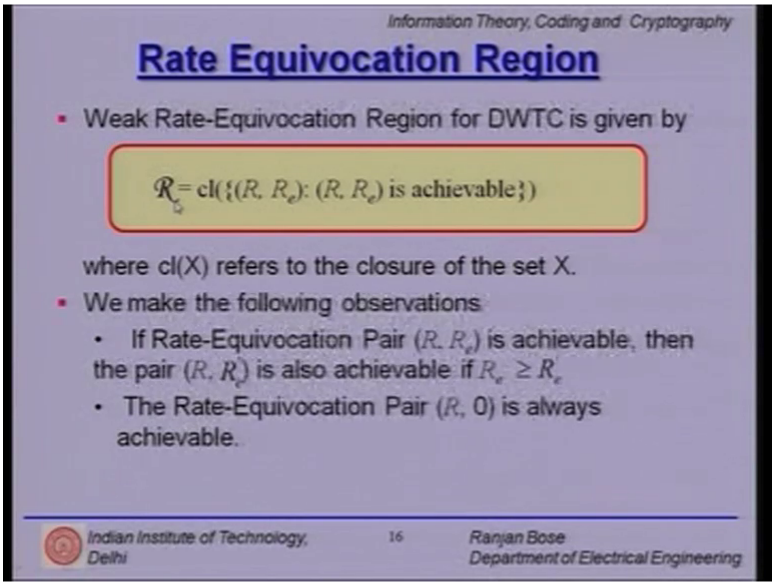
$$\lim_{n\to\infty} \frac{1}{n}E(C_n)\geq R_e$$

- The first condition is the **reliability condition** whereas the second condition pertains to the **weak secrecy condition**.
- Both these conditions may not get satisfied simultaneously.

Indian Institute of Technology, Delhi 15 Ranjan Bose Department of Electrical Engineering

Therefore, we had this pair and we talk about weak weight equivocation pair R comma R sub e and here we have these two condition; one is the reliability condition, the second is the weak secrecy condition. The first one limit tends to infinity probability of error for code word was to 0 and n tends to infinity 1 over n, the equivocation as a function of the code word should be greater than or equal to R e. Note both these condition may not get satisfied simultaneously.

(Refer Slide Time: 07:29)



Information Theory, Coding and Cryptography

Rate Equivocation Region

- Weak Rate-Equivocation Region for DWTC is given by

$$\mathcal{R} = \mathrm{cl}(\{(R, R_e): (R, R_e) \text{ is achievable}\})$$

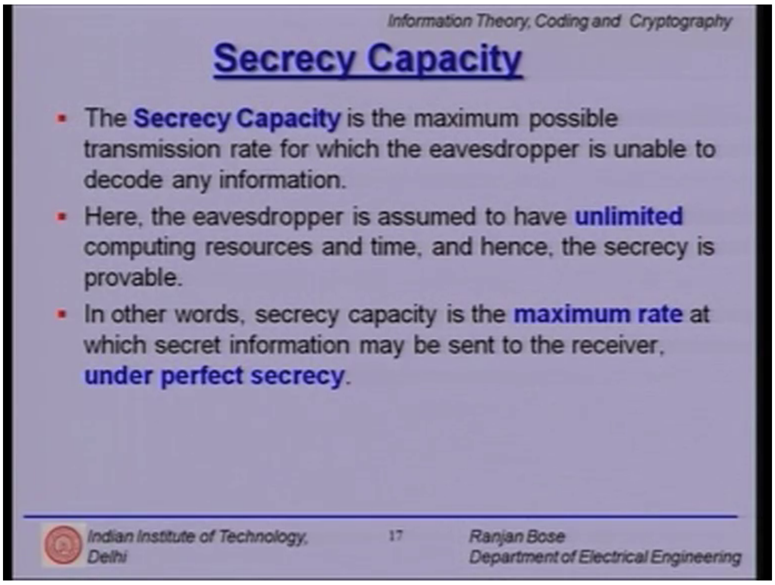
where cl(X) refers to the closure of the set X.

- We make the following observations
  - If Rate-Equivocation Pair (R, R_e) is achievable, then the pair (R, R_e) is also achievable if $R_e \geq R_e$
  - The Rate-Equivocation Pair $(R, 0)$ is always achievable.

Indian Institute of Technology, Delhi 16 Ranjan Bose Department of Electrical Engineering

Now, we also defined rate equivocation region plus time where the weak rate equivocation region for the degraded wiretap channel is given by R as the closure over the set R comma R e, where R comma R sub R e is achievable. So, we made the observations that the rate equivocation pair R comma R e is achievable then the rate pair R comma R e prime is also achievable, if R e is greater than or equal to R e prime. And clearly rate equivocation pair R comma 0 is always achievable.

(Refer Slide Time: 08:11)



Information Theory, Coding and Cryptography

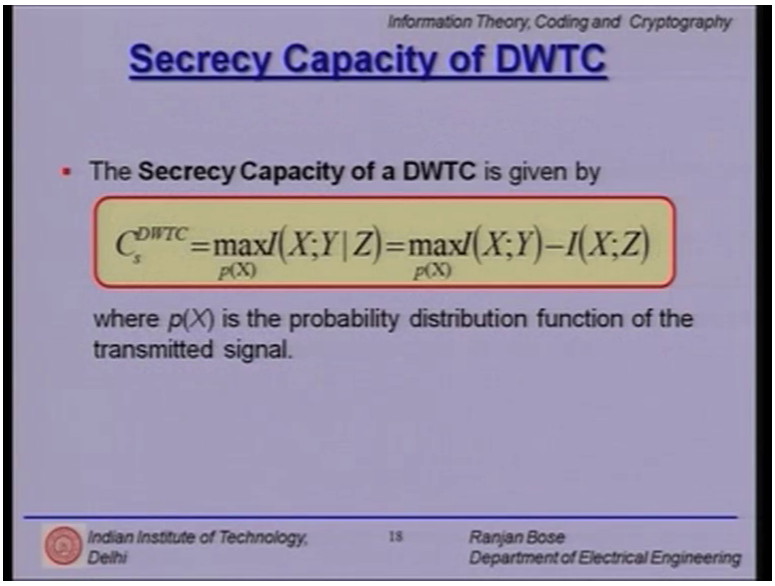
Secrecy Capacity

- The **Secrecy Capacity** is the maximum possible transmission rate for which the eavesdropper is unable to decode any information.
- Here, the eavesdropper is assumed to have **unlimited** computing resources and time, and hence, the secrecy is provable.
- In other words, secrecy capacity is the **maximum rate** at which secret information may be sent to the receiver, **under perfect secrecy**.

Indian Institute of Technology, Delhi 17 Ranjan Bose Department of Electrical Engineering

We had also defined secrecy capacity as maximum possible transmission rate for which the eavesdropper is unable to decode any information. What does it mean practically? Secrecy capacity is the maximum rate in which the secret information may be sent to the receiver under perfect secrecy.

(Refer Slide Time: 08:33)



Information Theory, Coding and Cryptography

Secrecy Capacity of DWTC

- The **Secrecy Capacity of a DWTC** is given by

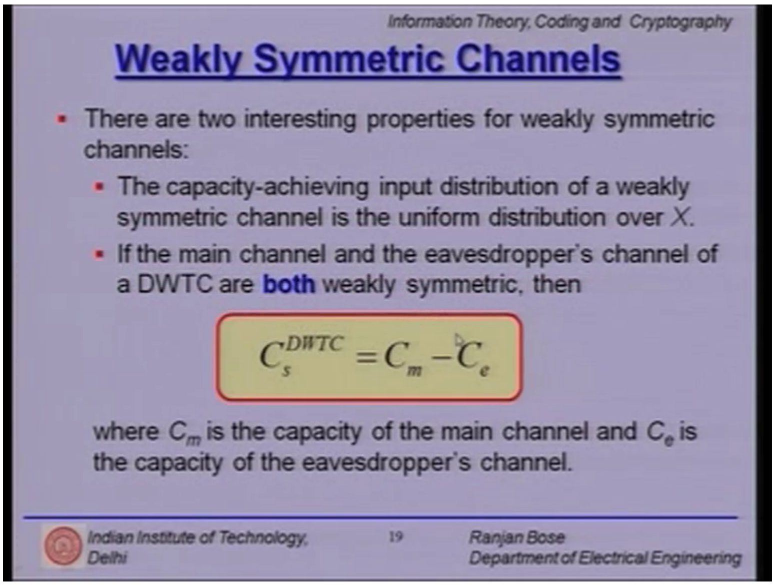
$$\boxed{C_s^{DWTC} = \max_{p(X)} I(X;Y|Z) = \max_{p(X)} I(X;Y) - I(X;Z)}$$

where $p(X)$ is the probability distribution function of the transmitted signal.

Indian Institute of Technology, Delhi 18 Ranjan Bose Department of Electrical Engineering

We had also defined secrecy capacity of the degraded wiretap channel as the difference between the mutual information I X semicolon Y and I X semicolon Z, where maximization is over the input probabilities. This is the secrecy capacity of a degraded wiretap channel.

(Refer Slide Time: 08:54)



Information Theory, Coding and Cryptography

Weakly Symmetric Channels

- There are two interesting properties for weakly symmetric channels:
  - The capacity-achieving input distribution of a weakly symmetric channel is the uniform distribution over X.
  - If the main channel and the eavesdropper's channel of a DWTC are **both** weakly symmetric, then

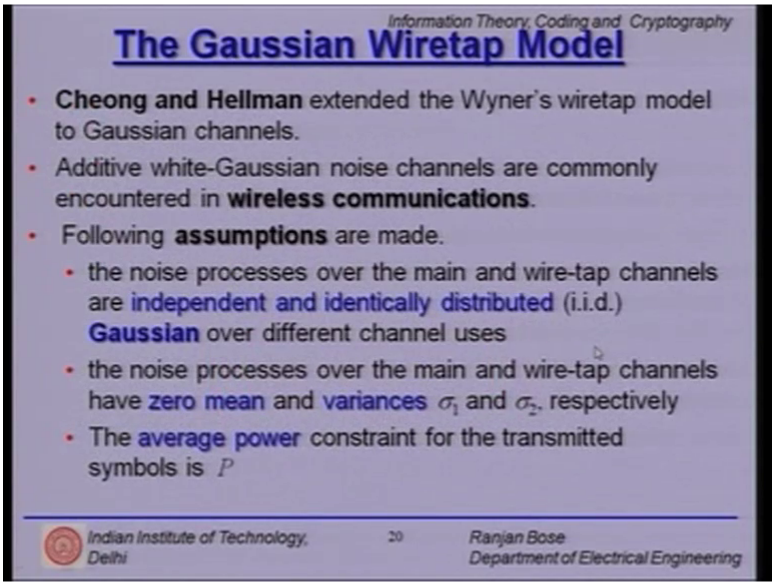
$$\boxed{C_s^{DWTC} = C_m - C_e}$$

where C_m is the capacity of the main channel and C_e is the capacity of the eavesdropper's channel.

Indian Institute of Technology, Delhi 19 Ranjan Bose Department of Electrical Engineering

We had also explained that if we have the luxury of both the main channel and the eavesdropper channel as weakly symmetric channel then the secrecy capacity of degraded wiretap channel in the special cases C m; the capacitor of the main channel minus C e the capacity of the eavesdropper channel. Please note: both the main channel and the eavesdropper channel must be weakly symmetric channels for this to happen.

(Refer Slide Time: 09:24)



Information Theory, Coding and Cryptography

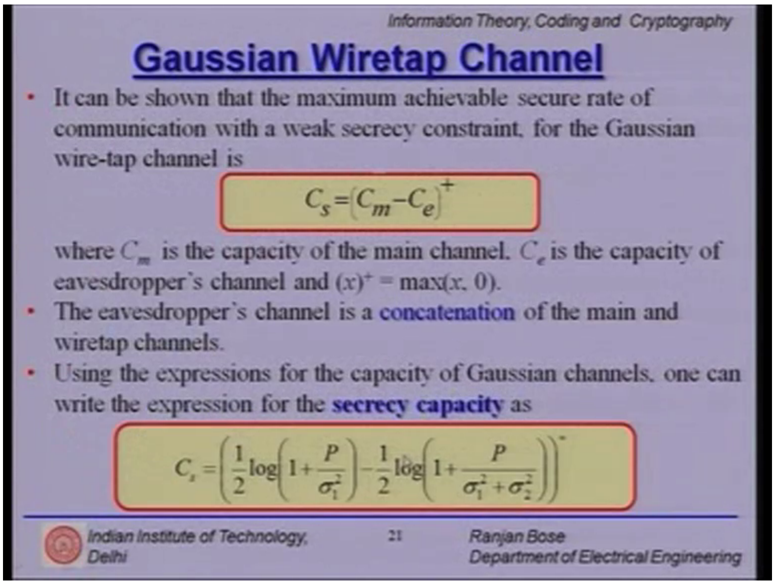
The Gaussian Wiretap Model

- **Cheong and Hellman** extended the Wyner's wiretap model to Gaussian channels.
- Additive white-Gaussian noise channels are commonly encountered in **wireless communications**.
- Following **assumptions** are made.
  - the noise processes over the main and wire-tap channels are independent and identically distributed (i.i.d.) **Gaussian** over different channel uses
  - the noise processes over the main and wire-tap channels have zero mean and variances σ_1 and σ_2, respectively
  - The average power constraint for the transmitted symbols is P

Indian Institute of Technology, Delhi 20 Ranjan Bose Department of Electrical Engineering

Then we talked about the Gaussian wiretap model, it was proposed by Cheong and Hellman. And, the assumptions were that the main channel and the wiretap channels were both independent and identically distributed Gaussian and their zero means and variances sigma 1 squared and sigma 2 squared whether average power constraint of P.

(Refer Slide Time: 09:47)



Information Theory, Coding and Cryptography

Gaussian Wiretap Channel

- It can be shown that the maximum achievable secure rate of communication with a weak secrecy constraint, for the Gaussian wire-tap channel is

$$C_s = (C_m - C_e)^+$$

where C_m is the capacity of the main channel. C_e is the capacity of eavesdropper's channel and $(x)^+ = \max(x, 0)$.
- The eavesdropper's channel is a concatenation of the main and wiretap channels.
- Using the expressions for the capacity of Gaussian channels, one can write the expression for the secrecy capacity as

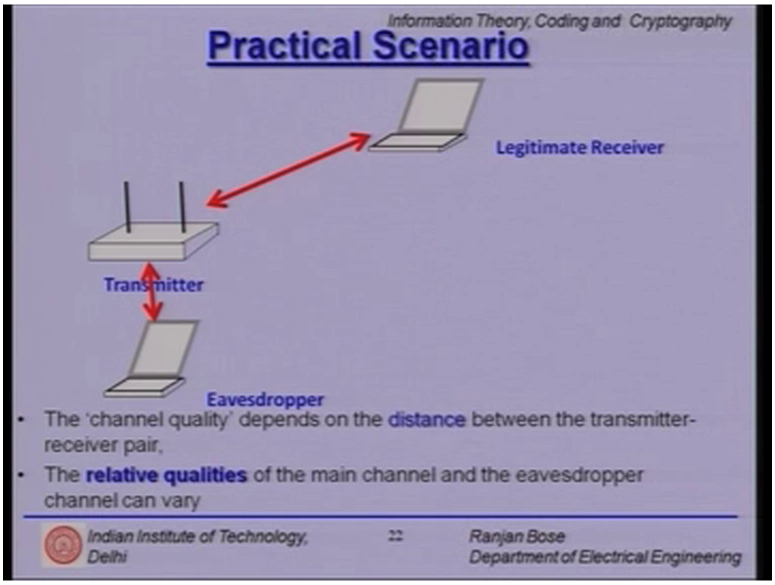
$$C_s = \left(\frac{1}{2}\log\left(1+\frac{P}{\sigma_1^2}\right) - \frac{1}{2}\log\left(1+\frac{P}{\sigma_1^2+\sigma_2^2}\right)\right)^+$$

Indian Institute of Technology, Delhi 21 Ranjan Bose Department of Electrical Engineering

In this case it was shown that the secrecy capacity is C m minus C e super plus where x super plus is nothing but max of x and zero so, it is non-negative. The eavesdropper channel is a concatenation of the main channel and the wiretap channel. Now, for the Gaussian case it is easy to plug in the value of C m the capacity of the main channel which is nothing but half log 1 plus power over SNR.

So, this is the capacity of the Gaussian channel for the main channel and here is the concatenation. So, you have 1 plus power over sigma 1 squared plus sigma 2 squared. So, the secrecy capacity C s is given by the difference between these to channel capacities.

(Refer Slide Time: 10:40)



Information Theory, Coding and Cryptography

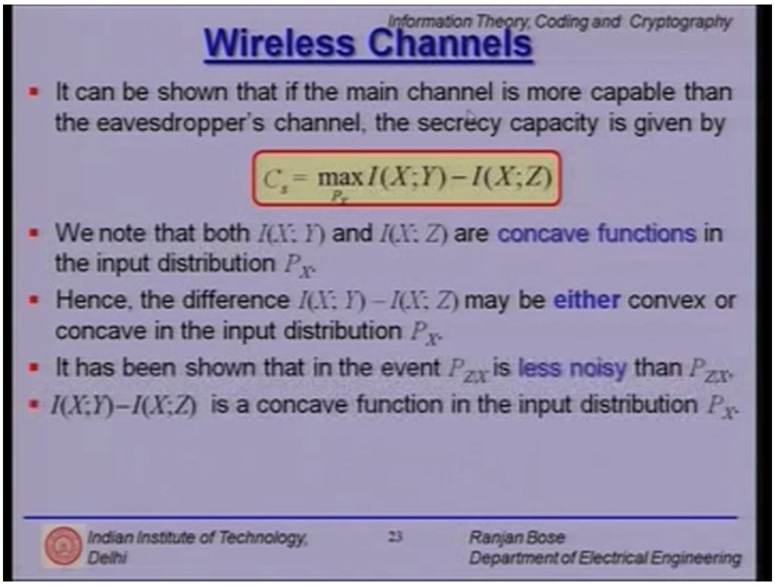
Practical Scenario

- The 'channel quality' depends on the **distance** between the transmitter-receiver pair.
- The **relative qualities** of the main channel and the eavesdropper channel can vary

Indian Institute of Technology, Delhi 22 Ranjan Bose Department of Electrical Engineering

Now, let us look at the practical scenario where we have a transmitter in the room and we have a legitimate receiver and before we realize we have an eavesdropper coming in. So, this is a democratic setup. So, both the legitimate receiver and the eavesdropper are free to move around in the room and it could be possible that the eavesdropper is closer to the transmitter than the legitimate receiver. But we know that the channel quality depends on the distance between the transmitter receiver pair. And so, the relative qualities of the main channel and eavesdropper channel can vary.

(Refer Slide Time: 11:19)



Information Theory, Coding and Cryptography

Wireless Channels

- It can be shown that if the main channel is more capable than the eavesdropper's channel, the secrecy capacity is given by

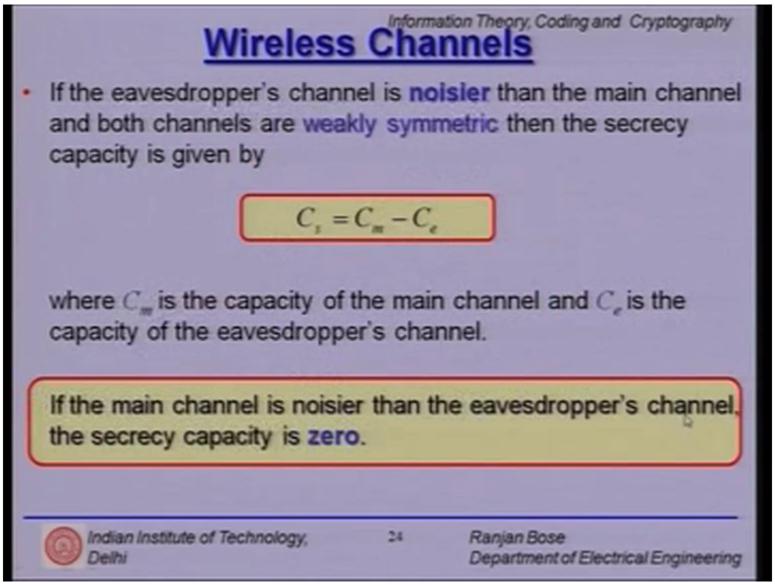
$$\boxed{C_s = \max_{P_x} I(X;Y) - I(X;Z)}$$

- We note that both $I(X;Y)$ and $I(X;Z)$ are **concave functions** in the input distribution P_X.
- Hence, the difference $I(X;Y) - I(X;Z)$ may be **either** convex or concave in the input distribution P_X.
- It has been shown that in the event P_{ZX} is **less noisy** than P_{ZX}.
- $I(X;Y)-I(X;Z)$ is a concave function in the input distribution P_X.

Indian Institute of Technology, Delhi 23 Ranjan Bose Department of Electrical Engineering

So, it can be shown that is the main channel is more capable than the eavesdropper channel then the secrecy capacity is given by C s is equal to maximization of over input probabilities I mutual information between X and Y minus I between X and Z. Now, note both I X semicolon Y and I X semicolon Z are concave functions in the input distribution of P X. Hence, the difference can either be convex or concave in the input distribution P X. It has been shown that in the event that P Z given X is less noisy then P Z given X. So, Z given Y is less noisy then Z given X then we have I X semicolon Y minus I X semicolon Z is necessarily a concave function in the input distribution of P of X.

(Refer Slide Time: 12:17)



Information Theory, Coding and Cryptography

Wireless Channels

- If the eavesdropper's channel is **noisier** than the main channel and both channels are weakly symmetric then the secrecy capacity is given by

$$\boxed{C_s = C_m - C_e}$$

where C_m is the capacity of the main channel and C_e is the capacity of the eavesdropper's channel.

If the main channel is noisier than the eavesdropper's channel, the secrecy capacity is **zero**.

Indian Institute of Technology, Delhi

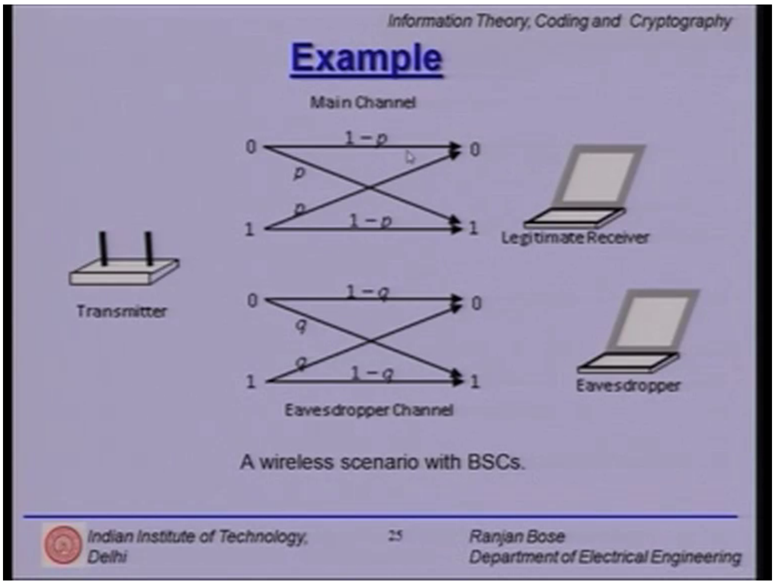
24

Ranjan Bose
Department of Electrical Engineering

So, what do we conclude is the eavesdropper channel is noisier than the main channel and both channels are weakly symmetric. In this special case the secrecy capacity is simply given by C s equal to the difference of C m, the capacitor of the main channel and C e, the capacity of the eavesdropper channel.

Now, if the main channel is noisier than the eavesdropper channel the secrecy capacity is clearly zero.

(Refer Slide Time: 12:51)


Information Theory, Coding and Cryptography

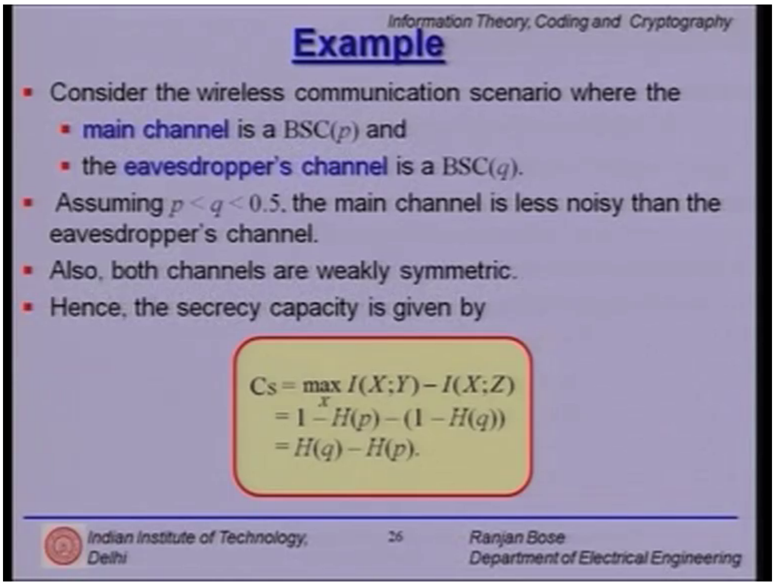
Example

A wireless scenario with BSCs.

Indian Institute of Technology, Delhi 25 Ranjan Bose Department of Electrical Engineering

Let us look at this practical example. So, we have a transmitter and it is happily communicating with the legitimate receiver and the channel which is the main channel is represented by this binary symmetric channel. Like it or not we have an eavesdropper in the room and it has another binary symmetric channel represented as follows; here the probability of error is small p, here it is small q.

(Refer Slide Time: 13:24)


Information Theory, Coding and Cryptography

Example

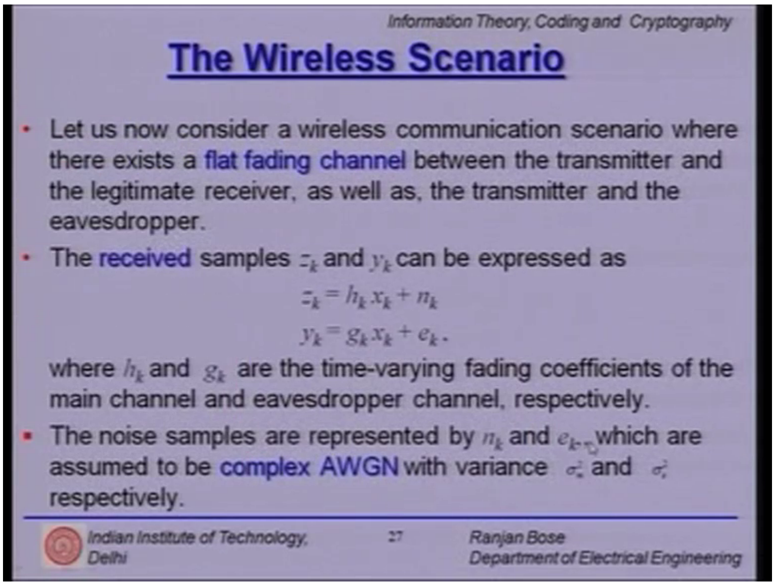
- Consider the wireless communication scenario where the
  - main channel is a $\mathrm{BSC}(p)$ and
  - the eavesdropper's channel is a $\mathrm{BSC}(q)$.
- Assuming $p < q < 0.5$, the main channel is less noisy than the eavesdropper's channel.
- Also, both channels are weakly symmetric.
- Hence, the secrecy capacity is given by

$$\begin{aligned} Cs &= \max_x I(X;Y) - I(X;Z) \\ &= 1 - H(p) - (1 - H(q)) \\ &= H(q) - H(p). \end{aligned}$$

Indian Institute of Technology, Delhi 26 Ranjan Bose Department of Electrical Engineering

So, the main channel is binary symmetric, the eavesdropper channel is binary symmetric both of them are weakly symmetric channel. Assuming p is less than q is less than 0.5, we make the main channel less noisy than the eavesdropper channel. So, if satisfied both the condition about main channel being less noisy than the eavesdropper channel and both channels are weakly symmetric channels. So, clearly the secrecy capacity is easily calculated as difference between the two mutual information. And we know that for this binary symmetric channel we have it is 1 minus H p minus 1 minus H q and it is nothing but H q minus H p; so very simple expression for this scenario.

(Refer Slide Time: 14:12)



Information Theory, Coding and Cryptography

The Wireless Scenario

- Let us now consider a wireless communication scenario where there exists a flat fading channel between the transmitter and the legitimate receiver, as well as, the transmitter and the eavesdropper.
- The received samples z_k and y_k can be expressed as

$$z_k = h_k x_k + n_k$$
$$y_k = g_k x_k + e_k.$$

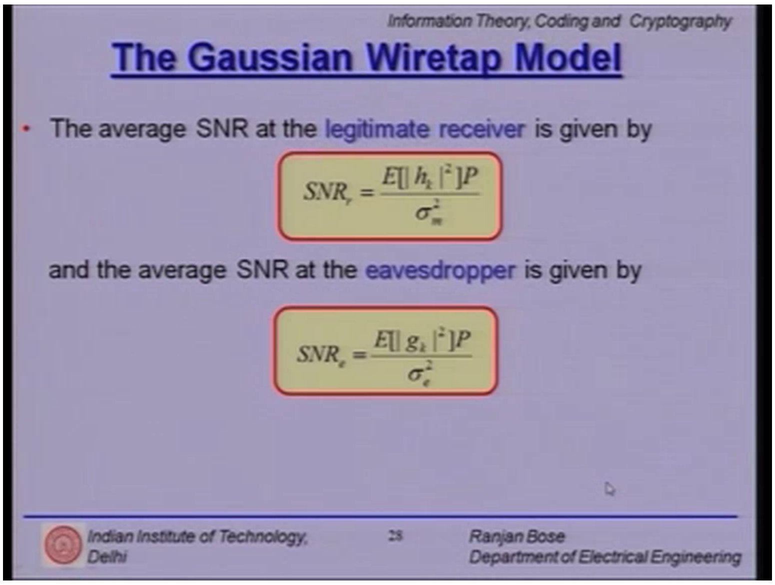
where h_k and g_k are the time-varying fading coefficients of the main channel and eavesdropper channel, respectively.

- The noise samples are represented by n_k and e_k, which are assumed to be complex AWGN with variance σ_m^2 and σ_e^2 respectively.

Indian Institute of Technology, Delhi 27 Ranjan Bose Department of Electrical Engineering

Now, let us considered the wireless scenario where flat fading occurs. So, there is flat fading between the transmitter and legitimate receiver as well as between the transmitter and eavesdropper. So, how does the received sample look like? Received samples can be expressed as z k is equal to this channel gain h k x k plus n k and y k is nothing but the channel gain g k x k plus e k; h k and g k are the time-varying fading coefficients of the main channel and the eavesdropper channel respectively. The noise samples are represented by n k and e k, which are assumed to be complex or additive white Gaussian with variance sigma m squared and sigma e squared respectively.

(Refer Slide Time: 15:00)



Information Theory, Coding and Cryptography

The Gaussian Wiretap Model

- The average SNR at the legitimate receiver is given by

$$SNR_r = \frac{E[|h_k|^2]P}{\sigma_m^2}$$

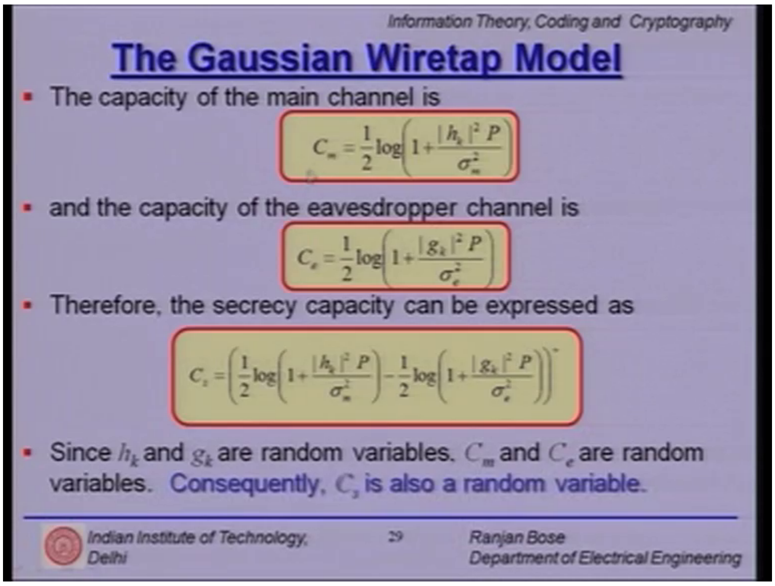
and the average SNR at the eavesdropper is given by

$$SNR_e = \frac{E[|g_k|^2]P}{\sigma_e^2}$$

Indian Institute of Technology, Delhi 28 Ranjan Bose Department of Electrical Engineering

So, it is easy to calculate the average SNR at the legitimate receiver, it is given by this expression and the average SNR at the eavesdropper is similarly given by SNR sub e with this expression ok. So, we have this expectation of the channel gain times the power normalized by the noise power.

(Refer Slide Time: 15:24)



Information Theory, Coding and Cryptography

The Gaussian Wiretap Model

- The capacity of the main channel is

$$C_m = \frac{1}{2}\log\left(1+\frac{|h_k|^2 P}{\sigma_m^2}\right)$$

- and the capacity of the eavesdropper channel is

$$C_e = \frac{1}{2}\log\left(1+\frac{|g_k|^2 P}{\sigma_e^2}\right)$$

- Therefore, the secrecy capacity can be expressed as

$$C_s = \left(\frac{1}{2}\log\left(1+\frac{|h_k|^2 P}{\sigma_m^2}\right) - \frac{1}{2}\log\left(1+\frac{|g_k|^2 P}{\sigma_e^2}\right)\right)^+$$

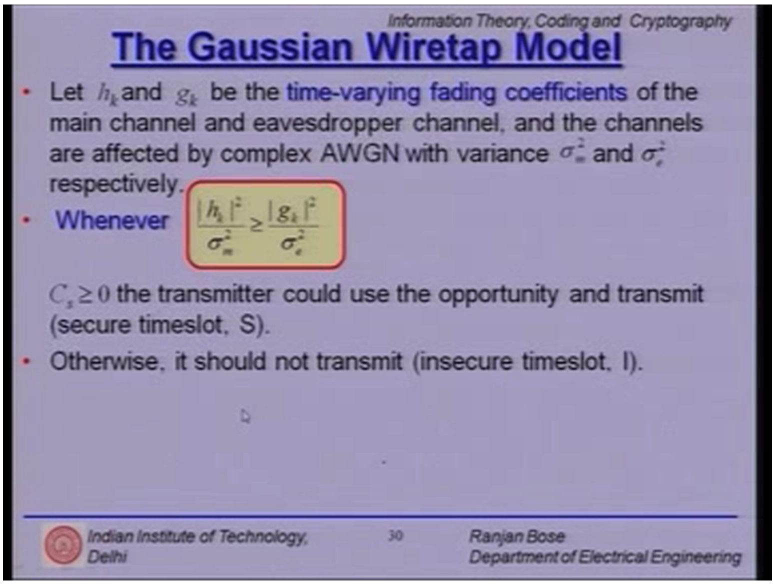
- Since h_k and g_k are random variables, C_m and C_e are random variables. Consequently, C_s is also a random variable.

Indian Institute of Technology, Delhi 29 Ranjan Bose Department of Electrical Engineering

So, the capacity of the main channel C m is simply plugging in the values in the expression for the capacity of the Gaussian channel because you are talking about the Gaussian channel here. And the capacity of eavesdropper channel is similarly like this ok, but we have not made any assumption about the wiretap model here it could be in general.

So, the capacity is nothing but the difference between the capacity of the main channel and the capacity of the eavesdropper channel right. Please note the super x here so, it can be greater than or equal to 0. But the interesting observation is that h of k and g of k are both random variables, consequently C m and C e are both random variables. Consequently the secrecy capacity is a random variable so, it keeps fluctuating.

(Refer Slide Time: 16:25)



Information Theory, Coding and Cryptography

The Gaussian Wiretap Model

- Let h_k and g_k be the time-varying fading coefficients of the main channel and eavesdropper channel, and the channels are affected by complex AWGN with variance σ_m^2 and σ_e^2 respectively.
- Whenever $\boxed{\frac{|h_k|^2}{\sigma_m^2} \ge \frac{|g_k|^2}{\sigma_e^2}}$

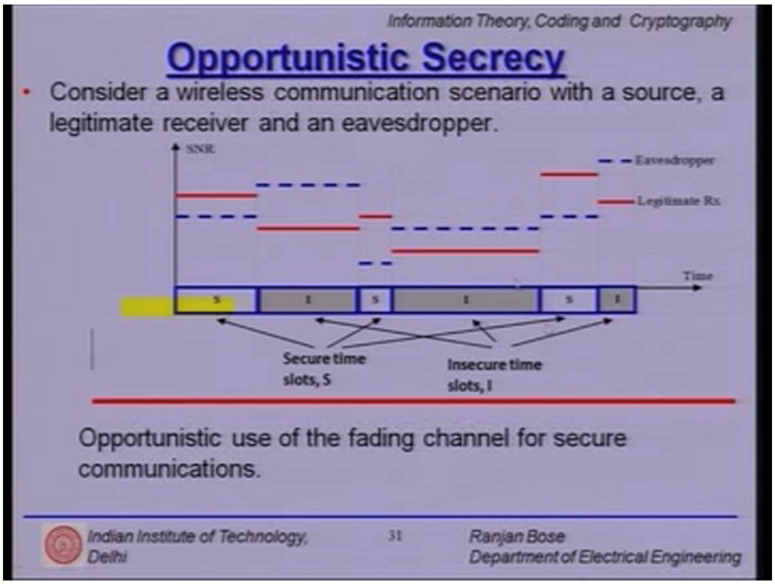
  $C_s \ge 0$ the transmitter could use the opportunity and transmit (secure timeslot, S).
- Otherwise, it should not transmit (insecure timeslot, I).

Indian Institute of Technology, Delhi 30 Ranjan Bose Department of Electrical Engineering

So, can we use to our benefit? So, h k and g k are time varying fading coefficients ok. So, whenever the SNR of the main channel is greater than the SNR of the eavesdropper channel we have an opportunity to get positive secrecy capacity.

So, let us talk about it in terms of a secure timeslot S and whenever it is less the main channel is poorer than the eavesdropper channel, we should not transmit. So, it is an insecure timeslot I.

(Refer Slide Time: 17:04)



Information Theory, Coding and Cryptography

Opportunistic Secrecy

- Consider a wireless communication scenario with a source, a legitimate receiver and an eavesdropper.

Opportunistic use of the fading channel for secure communications.

Indian Institute of Technology, Delhi

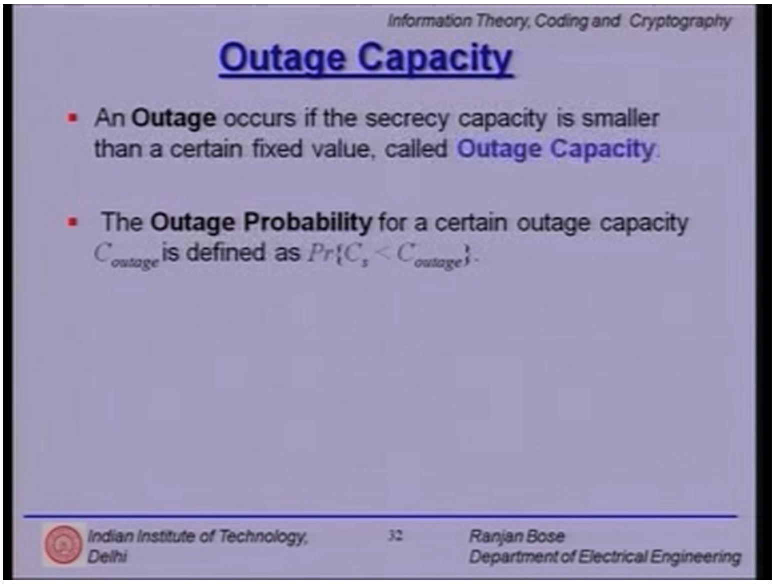
31

Ranjan Bose
Department of Electrical Engineering

So, suppose where the luxury to plot the received SNR of the legitimate receiver is the bold lines red. It is the received power of the legitimate and the dotted line represents the SNR at the eavesdropper.

So, sometimes the eavesdropper is better off, sometimes the main channel is better off. So, clearly whenever the signal strength and hence the SNR at legitimate received is better than that of the eavesdropper we have the secure timeslot S. If the things change then it is an in secured timeslot I and then sometimes it is secure insecure and so and so forth. So, we can use the fading channel opportunistically for secure communication.

(Refer Slide Time: 17:51)



Information Theory, Coding and Cryptography

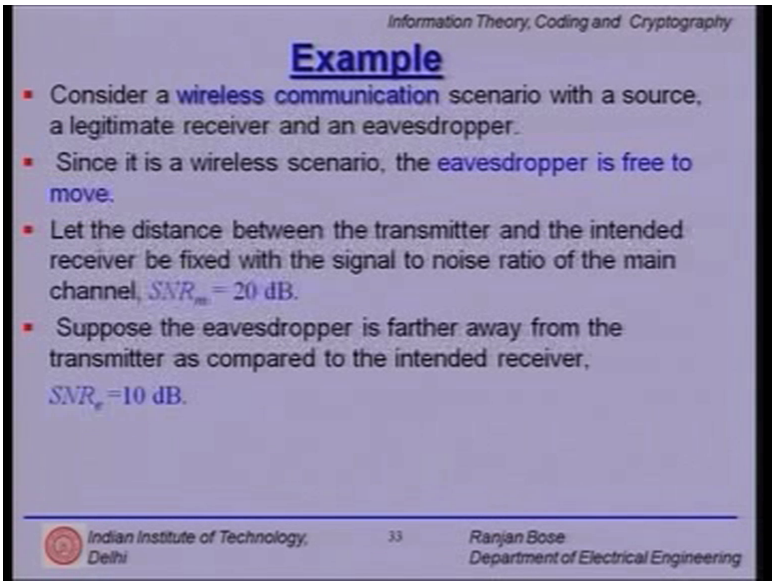
Outage Capacity

- An **Outage** occurs if the secrecy capacity is smaller than a certain fixed value, called Outage Capacity.
- The **Outage Probability** for a certain outage capacity C_{outage} is defined as $Pr\{C_s < C_{outage}\}$.

Indian Institute of Technology, Delhi 32 Ranjan Bose Department of Electrical Engineering

Now, let us define the outage capacity. First an outage occurs if the secrecy capacity is smaller than certain fixed value called outage capacity. And outage probability for a certain outage capacity C outage is defined as a probability C s is less than C outage. These are used to characterize and compare different secure communication schemes using physical layer security techniques.

(Refer Slide Time: 18:23)



Information Theory, Coding and Cryptography

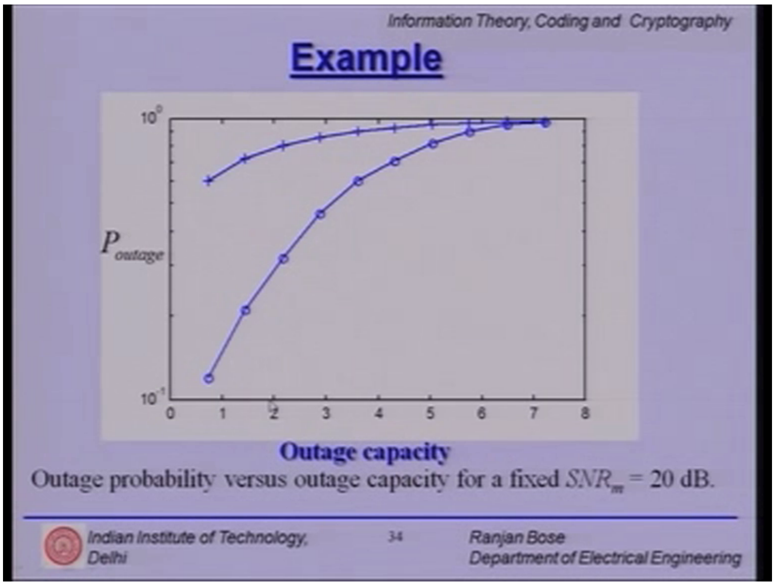
Example

- Consider a wireless communication scenario with a source, a legitimate receiver and an eavesdropper.
- Since it is a wireless scenario, the eavesdropper is free to move.
- Let the distance between the transmitter and the intended receiver be fixed with the signal to noise ratio of the main channel, $SNR_m = 20$ dB.
- Suppose the eavesdropper is farther away from the transmitter as compared to the intended receiver, $SNR_e = 10$ dB.

Indian Institute of Technology, Delhi 33 Ranjan Bose Department of Electrical Engineering

Now, consider of wireless communication scenario with source a legitimate receiver and an eavesdropper. And its wireless scenario it is completely democratic, the eavesdropper is free to move anywhere he or she wants to. So, in this example we say that the transmitter and the intended recipient are such that there SNR is fixed to 20 dB. But suppose the eavesdropper is farther away from the transmitter as compared to the intended receiving may be setting just outside the room and listening in so, SNR at the eavesdropper is poorer it is only 10 dB.

(Refer Slide Time: 19:00)



Information Theory, Coding and Cryptography

Example

Outage probability versus outage capacity for a fixed SNR_m = 20 dB.

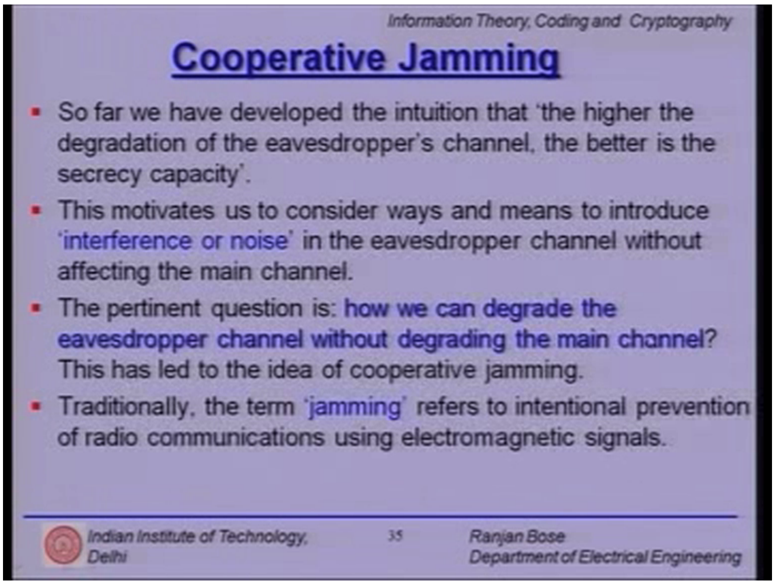
Indian Institute of Technology, Delhi

34

Ranjan Bose
Department of Electrical Engineering

So, you can plot the outage capacity as follows the x axis versus the P outage on this site and you can see that the outage probability versus the outage capacity for a fixed SNR of the main channel at 20 dB.

(Refer Slide Time: 19:20)



Information Theory, Coding and Cryptography

Cooperative Jamming

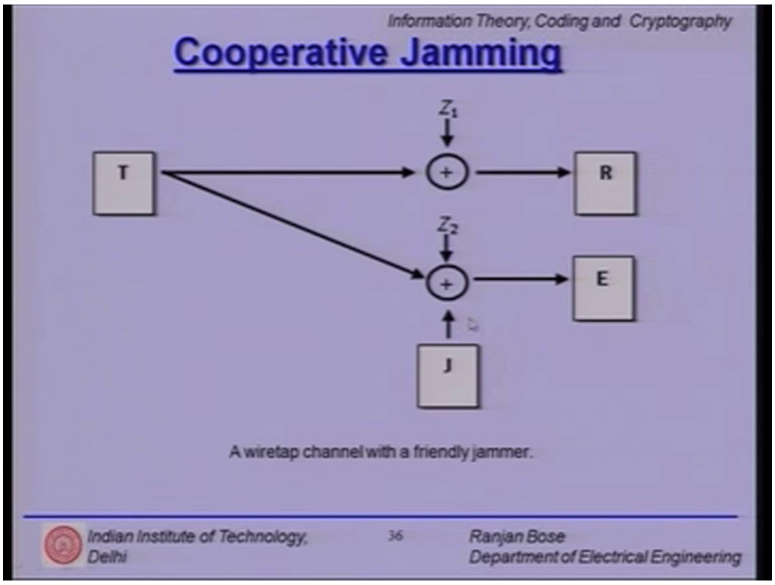
- So far we have developed the intuition that 'the higher the degradation of the eavesdropper's channel, the better is the secrecy capacity'.
- This motivates us to consider ways and means to introduce 'interference or noise' in the eavesdropper channel without affecting the main channel.
- The pertinent question is: how we can degrade the eavesdropper channel without degrading the main channel? This has led to the idea of cooperative jamming.
- Traditionally, the term 'jamming' refers to intentional prevention of radio communications using electromagnetic signals.

Indian Institute of Technology, Delhi 35 Ranjan Bose Department of Electrical Engineering

Now, we will look at couple of practical techniques to help physical layer security. What is the motivation? So, far we have developed the intuition that higher the degradation of the eavesdropper channel the better is the secrecy capacity. So, should we just relay on the channel or can we do something to degrade the channel of the eavesdropper. So, we would like to introduce some interference or artificial noise in eavesdropper channel without affecting the main channel.

So, how can we degrade the eavesdropper channel without degrading the main channel that is the million-rupee question. This has led to the idea of cooperative jamming, where the term 'jamming' refers to intentional prevention of radio communication using electromagnetic signals.

(Refer Slide Time: 20:16)



Information Theory, Coding and Cryptography

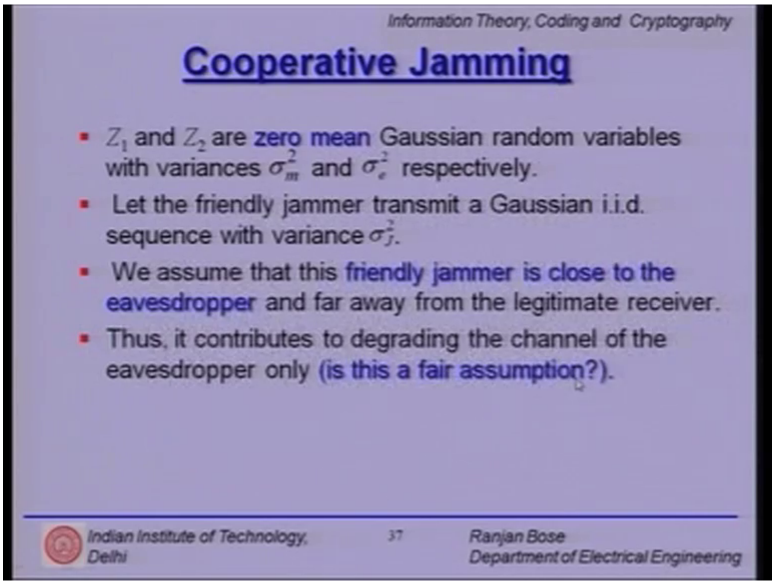
Cooperative Jamming

A wiretap channel with a friendly jammer.

Indian Institute of Technology, Delhi 36 Ranjan Bose Department of Electrical Engineering

So, considered the signal scenario where we have a transmitter which is our source, it sense information to our legitimate receiver R and it is a noisy channel so, Z 1 is the noise been added. As always we have friend the eavesdropper sitting in the room and it also receive signal and the noise added is Z 2. The idea is can we have friendly jammer who is only affecting the eavesdropper, but not the intended recipient directly. This is the basic idea about cooperating jamming. So, is jammer is adding additional interference to the eavesdropper's channel thereby degrading it, thereby improving the secrecy capacity of the system.

(Refer Slide Time: 21:09)



Information Theory, Coding and Cryptography

Cooperative Jamming

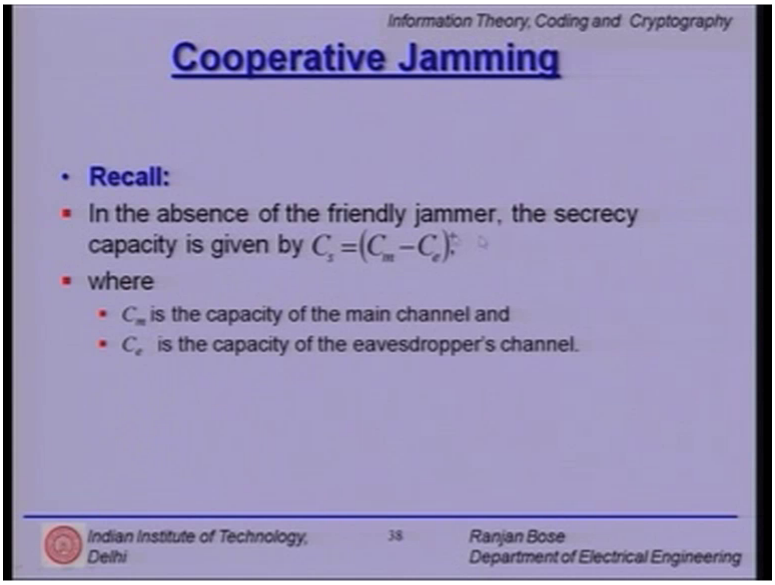
- Z_1 and Z_2 are zero mean Gaussian random variables with variances σ_m^2 and σ_e^2 respectively.
- Let the friendly jammer transmit a Gaussian i.i.d. sequence with variance σ_J^2.
- We assume that this friendly jammer is close to the eavesdropper and far away from the legitimate receiver.
- Thus, it contributes to degrading the channel of the eavesdropper only (is this a fair assumption?).

Indian Institute of Technology, Delhi 37 Ranjan Bose Department of Electrical Engineering

So, in this simple set up Z 1 and Z 2 or zero mean with variances sigma m squared and sigma e squared. And let the friendly jammer transport also Gaussian i.i.d. sequence with variance sigma j squared.

So, we assume that the friendly jammer has quietly place itself close to the eavesdropper and quite far away from the legitimate receiver right. Now, we are not discussing the fairness of this assumption, but less assume that it has been able to do it. Maybe it has a directional antenna, maybe it is using some technique, but this is other assumptions.

(Refer Slide Time: 21:44)



Information Theory, Coding and Cryptography

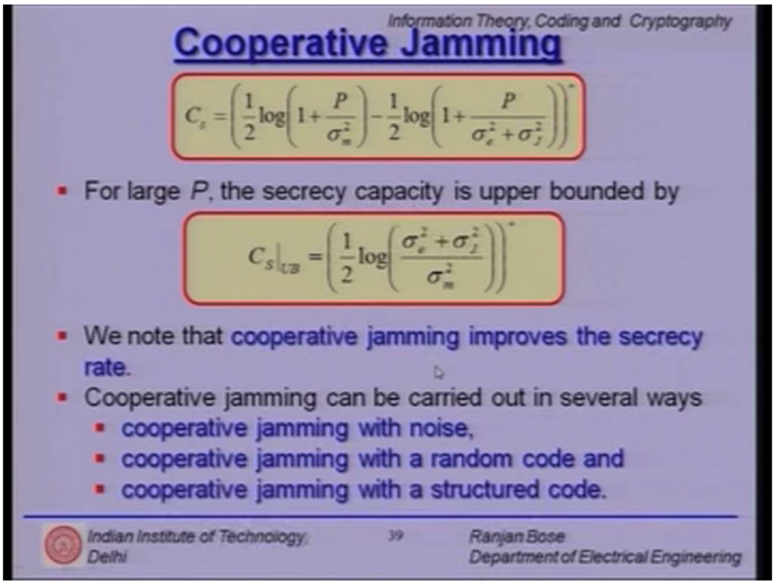
Cooperative Jamming

- **Recall:**
- In the absence of the friendly jammer, the secrecy capacity is given by $C_s = (C_m - C_e)^+$
- where
  - C_m is the capacity of the main channel and
  - C_e is the capacity of the eavesdropper's channel.

Indian Institute of Technology, Delhi 38 Ranjan Bose Department of Electrical Engineering

So, we recall that in the absence of the friendly jammer the secrecy capacity was simply C s equal to C m minus C e provided we had the certain conditions being satisfied. Here C m is the main channel capacity, C e is eavesdropper channel capacity.

(Refer Slide Time: 22:01)



Information Theory, Coding and Cryptography

Cooperative Jamming

$$C_s = \left(\frac{1}{2}\log\left(1+\frac{P}{\sigma_m^2}\right) - \frac{1}{2}\log\left(1+\frac{P}{\sigma_e^2+\sigma_J^2}\right)\right)^+$$

- For large *P*, the secrecy capacity is upper bounded by

$$C_S\big|_{UB} = \left(\frac{1}{2}\log\left(\frac{\sigma_e^2+\sigma_J^2}{\sigma_m^2}\right)\right)^+$$

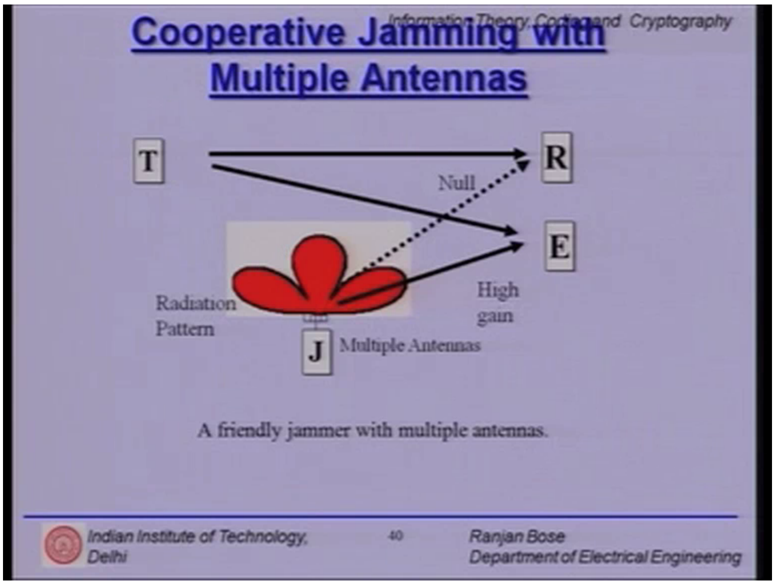
- We note that cooperative jamming improves the secrecy rate.
- Cooperative jamming can be carried out in several ways
  - cooperative jamming with noise,
  - cooperative jamming with a random code and
  - cooperative jamming with a structured code.

Indian Institute of Technology Delhi 39 Ranjan Bose Department of Electrical Engineering

So, when we have the cooperative jamming the main channel is unaffected, but the eavesdropper channel has the noise power and the jamming power put together. And when we make P very large, then the upper bounded C s P vanishes and we are left with half log; in the numerator sigma e square plus sigma j square, plus sigma j squared is the noise power introduced by the jammer whereas, sigma m squared is the noise power in the main channel.

So, clearly the numerator is larger and it can be made as larger possible depending upon how much power we want to give to the jammer and cooperative jammer can improve secrecy rate. There are many ways to do cooperative jamming and some of the ways are cooperative jamming with noise, cooperative jamming with random code and cooperative jamming with structured codes.

(Refer Slide Time: 23:03)



Information Theory Coding and Cryptography

Cooperative Jamming with Multiple Antennas

T

R

Null

E

Radiation Pattern

High gain

J

Multiple Antennas

A friendly jammer with multiple antennas.

Indian Institute of Technology, Delhi

40

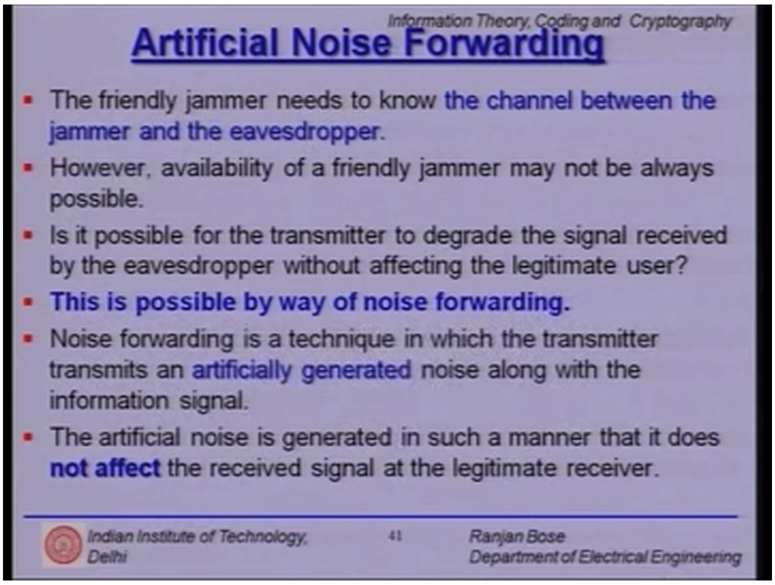
Ranjan Bose
Department of Electrical Engineering

Now, if we have the luxury of multiple antennas we can do cooperative jamming using that. So, scenario is similar we have our transmitter R legitimate receiver and omnipresent eavesdropper is always trying to listen in. Of course, we introduced the new player J which is a friendly jammer and it has multiple antennas. So, multiple antennas allow you to radiate power differential in certain directions, it can form a beam pattern and it can direct the beam at certain directions.

So, suppose this is the radiation pattern and by changing the weights on the antenna elements I can steer this beam. So, if my receiver or the eavesdropper move around in the room my friend the friendly jammer can steer the beam accordingly. But what does do with the beam? Well it makes the radiation pattern such then there is high gain in the direction of the eavesdropper, but there is null in the direction of the legitimate receiver.

So, very little of the jamming sequence is actually received by the legitimate receiver, but the maximum brand of the jamming signal is bond by the eavesdropper thereby degrading its channel. So, this is one of the simple techniques of cooperative jamming with multiple antennas at the friendly jammer. Another technique that can be used for physical layer security is called artificial noise forward forwarding.

(Refer Slide Time: 24:37)



Information Theory, Coding and Cryptography

Artificial Noise Forwarding

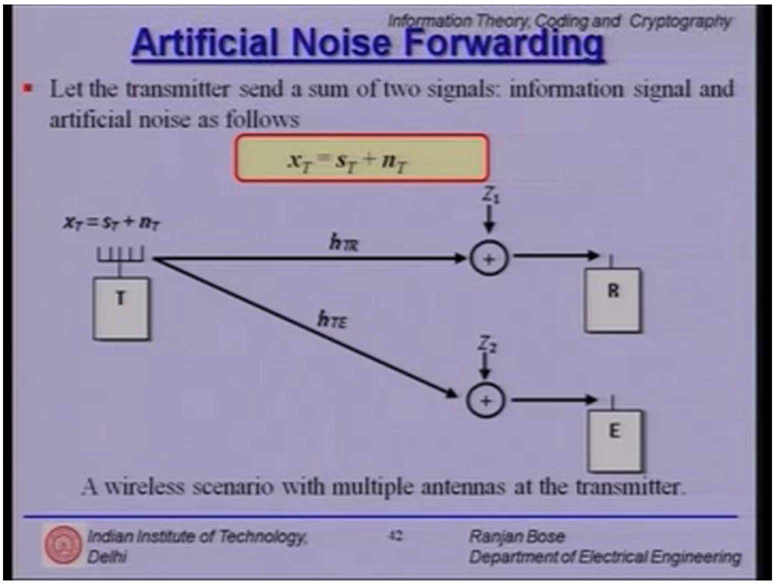
- The friendly jammer needs to know the channel between the jammer and the eavesdropper.
- However, availability of a friendly jammer may not be always possible.
- Is it possible for the transmitter to degrade the signal received by the eavesdropper without affecting the legitimate user?
- **This is possible by way of noise forwarding.**
- Noise forwarding is a technique in which the transmitter transmits an artificially generated noise along with the information signal.
- The artificial noise is generated in such a manner that it does **not affect** the received signal at the legitimate receiver.

Indian Institute of Technology, Delhi 41 Ranjan Bose Department of Electrical Engineering

Now, the friendly jammer in the earlier example needs to know the channel between the jammer and the eavesdropper or maybe the location of the eavesdropper, but it is not always available. Question is, is it possible for the transmitter to degrade the signal received by the eavesdropper without affecting the legitimate user and this is possible by way of noise forwarding.

So, noise forwarding is technique in which the transmitter transmits an artificially generated noise along with information signal. This artificial noise is generated in such manner that they does not affect the received signal. Most rarely the legitimate receiver who is our friend should be able to cancel out this noise, but our eavesdropper will not be able to cancel it out.

(Refer Slide Time: 25:33)



Information Theory, Coding and Cryptography

Artificial Noise Forwarding

- Let the transmitter send a sum of two signals: information signal and artificial noise as follows

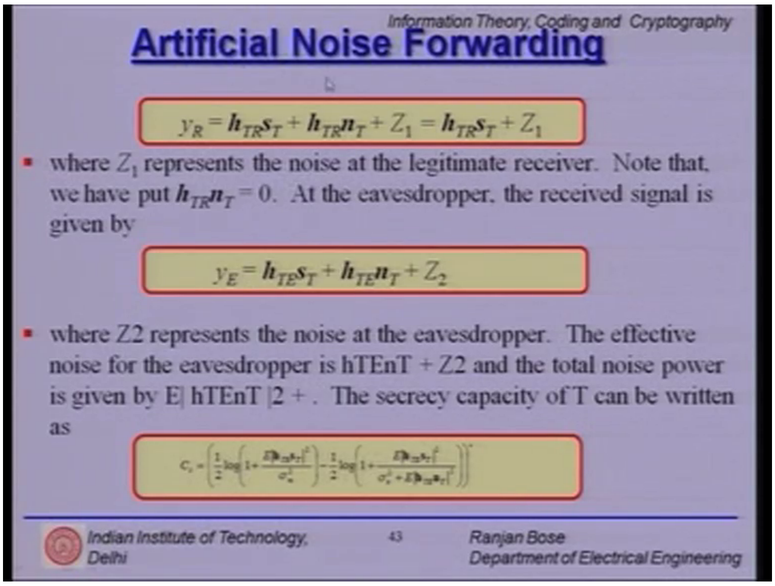
$$x_T = s_T + n_T$$

A wireless scenario with multiple antennas at the transmitter.

Indian Institute of Technology, Delhi 42 Ranjan Bose Department of Electrical Engineering

So we have transmitter, we have a channel to the legitimate receiver with channel gain, and we have channel to the eavesdropper and again as before we have additive white Gaussian noise.

(Refer Slide Time: 25:49)



Information Theory, Coding and Cryptography

Artificial Noise Forwarding

$$y_R = \boldsymbol{h}_{TR}\boldsymbol{s}_T + \boldsymbol{h}_{TR}\boldsymbol{n}_T + Z_1 = \boldsymbol{h}_{TR}\boldsymbol{s}_T + Z_1$$

- where Z_1 represents the noise at the legitimate receiver. Note that, we have put $\boldsymbol{h}_{TR}\boldsymbol{n}_T = 0$. At the eavesdropper, the received signal is given by

$$y_E = \boldsymbol{h}_{TE}\boldsymbol{s}_T + \boldsymbol{h}_{TE}\boldsymbol{n}_T + Z_2$$

- where Z2 represents the noise at the eavesdropper. The effective noise for the eavesdropper is hTEnT + Z2 and the total noise power is given by E| hTEnT |2 + . The secrecy capacity of T can be written as

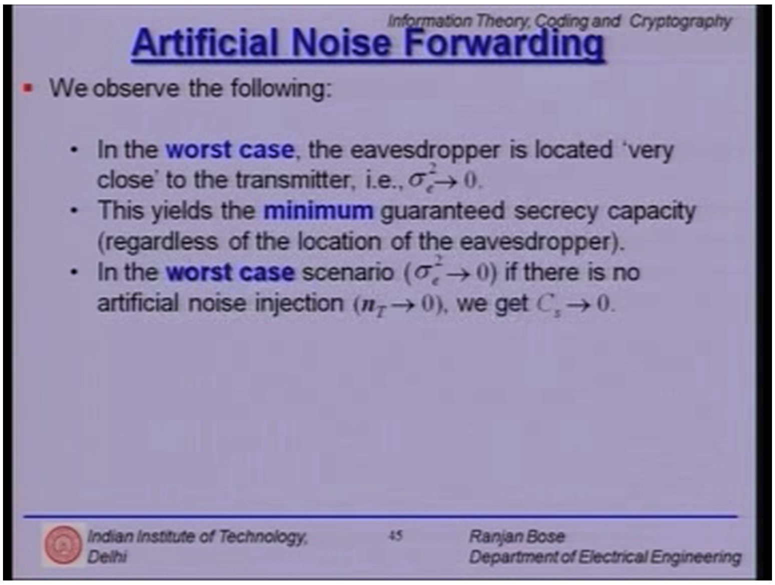
$$C_s = \left(\frac{1}{2}\log\left(1+\frac{E|\boldsymbol{h}_{TR}\boldsymbol{s}_T|^2}{\sigma_n^2}\right) - \frac{1}{2}\log\left(1+\frac{E|\boldsymbol{h}_{TE}\boldsymbol{s}_T|^2}{\sigma_e^2 + E|\boldsymbol{h}_{TE}\boldsymbol{n}_T|^2}\right)\right)^+$$

Indian Institute of Technology, Delhi 43 Ranjan Bose Department of Electrical Engineering

So, here you can write the expression for the signal received at the legitimate receiver y R which is basically the gain in terms of h TR s T h TR n T and Z 1, which can be clubbed as follows right. The Z 1 is represents the noise at the legitimate receiver, but note that h TR n T which is the jamming signal received the artificial noise received at the legitimate receiver is cancelled out because we have some techniques to cancel out the noise ok.

So, this is the artificially generated noise term. This vanishes from the expression for the legitimate receiver, but it stays (Refer Time: 26:38) for the expression of the eavesdropper. So, this dropping signal receives the transmitted signal, the transmitted artificial noise and its local noise. So, the secrecy capacity again can be written as a difference between the main channel and the eavesdropper as follows.

(Refer Slide Time: 27:05)



Information Theory, Coding and Cryptography

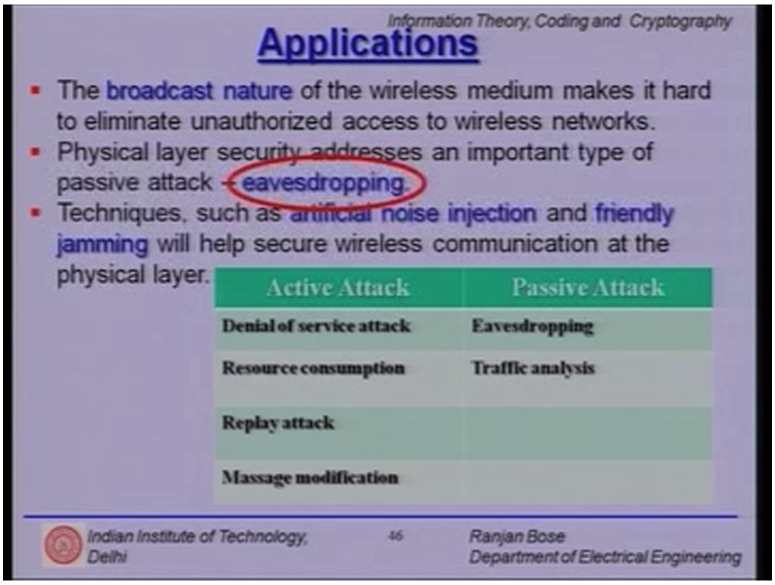
Artificial Noise Forwarding

- We observe the following:
    - In the **worst case**, the eavesdropper is located 'very close' to the transmitter, i.e., $\sigma_e^2 \to 0$.
    - This yields the **minimum** guaranteed secrecy capacity (regardless of the location of the eavesdropper).
    - In the **worst case** scenario ($\sigma_e^2 \to 0$) if there is no artificial noise injection ($n_T \to 0$), we get $C_s \to 0$.

Indian Institute of Technology, Delhi 45 Ranjan Bose Department of Electrical Engineering

So, we observe the following. The eavesdropper if located very close to the transmitter that is if sigma e squared goes to 0; this gives the minimum guaranteed secrecy capacity regardless of the location the eavesdropper. Because we have to taken into consider consideration the worst case scenario and the eavesdropper is placed very close to the transmitter. So, all the secrecy is provided by the artificial noise introduced by the channel.

(Refer Slide Time: 27:39)



Information Theory, Coding and Cryptography

Applications

- The broadcast nature of the wireless medium makes it hard to eliminate unauthorized access to wireless networks.
- Physical layer security addresses an important type of passive attack – eavesdropping.
- Techniques, such as artificial noise injection and friendly jamming will help secure wireless communication at the physical layer.

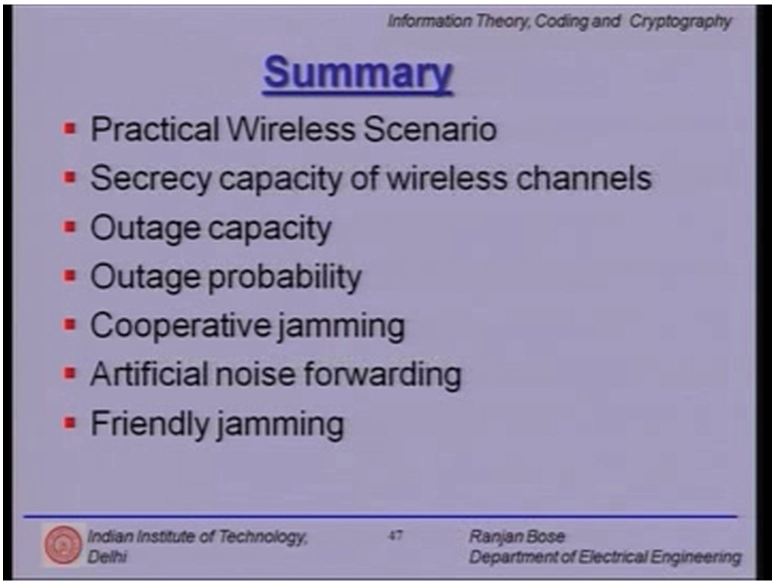
Active Attack	Passive Attack
Denial of service attack	Eavesdropping
Resource consumption	Traffic analysis
Replay attack	
Massage modification	

Indian Institute of Technology, Delhi 46 Ranjan Bose Department of Electrical Engineering

So, we try to conclude this lecture with some applications. Please note that the broadcast nature of the wireless medium makes it very hard to eliminate unauthorized access to wireless networks. People can be standing outside the room and listening in, they can be sitting in cars parked outside the house and listening in. In office scenario, home scenario it becomes very difficult to get rid of eavesdropping; physical layer security addresses this problem. So, this passive attack eavesdropping is primarily addressed by this physical layer security.

If you look at the kinds of popular attack, we have denial of service attack, resource consumption attack, replay attack and message modification attack these are the active attacks. Eavesdropping on the other hand is passive attack, as is traffic analysis. So, R physical layer security techniques are pretty much useful for eavesdropping kind of attacks. And techniques such as artificial noise injection, friendly jamming etcetera will help reduce wireless communication problems in terms of security at the physical layer. We are not making any assumption what kind of resources are available at the eavesdropper or how much computing power or time it has, ok.

(Refer Slide Time: 29:16)



Information Theory, Coding and Cryptography

Summary

- Practical Wireless Scenario
- Secrecy capacity of wireless channels
- Outage capacity
- Outage probability
- Cooperative jamming
- Artificial noise forwarding
- Friendly jamming

Indian Institute of Technology, Delhi 47 Ranjan Bose Department of Electrical Engineering

So, let us summaries this lecture. We started off with practical wireless scenarios and talked about physical layer security in real life wireless scenarios. We talked about the secrecy capacity of wireless channels. We talked about outage capacity and outage probability, these are used to characterize systems and compare system using physical layer techniques. Then we talked about couple of practical techniques, we started off with cooperative jamming, artificial noise forwarding and friendly jamming.

That brings us to the end of this lecture.