Using Channel Noise for Information theoretic Security

P Vidyadhar Rao

Research in Information Security

December 8, 2013

Information Theoretic Security

Assumption 1

Alice and Bob share a secret key K

Assumption 2

Bob and Eve have perfect access to the insecure channel

Definition

Shannon's perfect secrecy: $I(M; C) = 0$

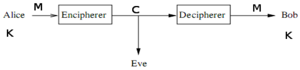

Figure: Shannon's model [Sha49]

Theorem

Perfect secrecy is achievable iff $H(K) \geq H(M)$

Remark

Perfect secrecy is unachievable in practice!

Using channel noise

Assumption 1

Alice and Bob do not share secret keys

Assumption 2

Alice-Bob communicate over main channel

Assumption 3

Eve has access to messages over wiretap channel

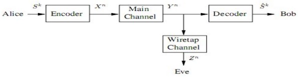

Figure: Wiretap Channel Model [Wyn75]

Challenge

Is it possible to communicate at a transmission rate R with small error-rate, while keeping Eve with no significant information about messages sent over main channel?

Definition

For $R > 0$ and $d > 0$, pair (R, d) is achievable if, $\forall \epsilon > 0$, $\exists (k, n, \Delta, P_e)$ encoder-decoder s.t:

- $k.\frac{H_S}{n} \geq R - \epsilon$
- $\Delta \geq d - \epsilon$, *where* $\Delta = \frac{1}{k} H(S^k | Z^n)$.
- $P_e \leq \epsilon$, *where* $P_e = \frac{1}{k} \sum_{i=1}^{k} P(S_i \neq \hat{S}_i)$.

Let $p_X(x), x \in X$ be a probability mass function and $P(R)$ denote the set of all distributions p_X s.t $I(X; Y) \geq R$.

For $0 \leq R \leq C_M$, let $\Gamma(R) = sup_{p_X \in P(R)} I(X; Y|Z) = sup_{p_X \in P(R)} [I(X; Y) - I(X; Z)]$.

Theorem

Wyner's main result on the set of all acheivable pairs is given by

$\Re = \left\{ (R, d) : 0 \leq R \leq C_M, 0 \leq d \leq H_S, \frac{d}{H_S} \leq \frac{\Gamma(R)}{R} \right\}$

Definition

The secrecy capacity of the channel pair (Q_M, Q_W) *is defined by* $C_S = max_{(R,H_S)\in\Re} R.$

Theorem

If $C_M > C_{MW}$, $\exists$ *unique solution* C_S *of* $C_S = \Gamma(C_S)$. *Further,* C_S *is the maximum* R *s.t* $(R, H_S) \in \Re$ *and satisfies*
$0 < C_M - C_{MW} \leq \Gamma(C_M) \leq C_S \leq C_M.$

Remark

Here, it requires that $C_M > C_{MW}$ *to have strictly positive secrecy capacity i.e., in order to be able to communicate with perfect secrecy, Alice and Bob must have a better channel than the wiretap channel.*

Using public insecure channel

Assumption 1

Alice-Bob share a small key required for authentication in the public channel.

Assumption 2

Eve can listen to the communication over public channel, but cannot perform an identity spoofing attack.

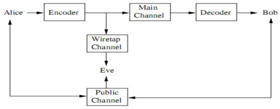

Figure: Broadcast channel with a public channel [Mau93]

Challenge

To acheive strictly positive secrecy capacity, even if Eves channel is better than main channel.

General Key Agreement protocol

- Alice, Bob and Eve know random variables X, Y and Z with joint probability distribution P_{XYZ}.
- Alice and Bob share no secrect key initially, other than a short key required for authentication in the public channel.
- Eve knows the protocol and the codes used.
- Alice sends messages at odd steps $[C_1, C_3, \ldots]$.
- Bob sends messages at even steps $[C_2, C_4, \ldots]$.
- At the end of t-steps,
  - Alice computes secret key S as a function of X and $C^t = [C_1, C_2, \ldots]$
  - Bob computes secret key $S^{'}$ as a function of Y and C^t

Definition

A secret key agreement protocol is (ϵ, δ)*-secure if, for some specified (small)* ϵ *and* δ*, satisfies:*

1. *For odd* i, $H(C_i|C^{i-1}X) = 0$*; and for even* i, $H(C_i|C^{i-1}Y) = 0$*;*
2. $H(S|C^tX) = 0$*; and* $H(S^{'}|C^tY) = 0$*;*
3. $P(S \neq S^{'}) \leq \epsilon$*;*
4. $I(S; C^tZ) \leq \delta$*;*

The secret key rate, denoted $S(X; Y||Z)$*, is the maximum rate* R *s.t,* $\forall \epsilon > 0$, $\exists$ *a protocol, for sufficiently large* n*, that satisfies:*

- *conditions 1-3*
- $\frac{1}{n} I(S; C^tZ) \leq \epsilon$*;*
- $\frac{1}{n} H(S) \geq R - \epsilon$

Theorem

For discrete memoryless channels, the secret key rate $S(X;Y||Z)$ *is shown to satisfy:*

$$max[I(Y;X) - I(Z;X), I(X;Y) - I(Z;Y)] \leq S(X;Y||Z) \leq min[I(X;Y), I(X;Y|Z)];$$

For a general broadcast channels, specified by $P(YZ|X)$*, the secrecy capacity,* $\hat{C}(P_{YZ|X})$*, is shown to satisfy:*

$$max_{P_X} S(X;Y||Z) \leq \hat{C}(P_{YZ|X}) \leq min[max_{P_X} I(X;Y), max_{P_X} I(X;Y|Z)].$$

Remark

If Eve has less information about Y *than Alice or less information about* X *than Bob, then such a difference of information can be exploited.*
Even if the eavesdropper has a better channel than the legitimate users, perfect secure communication can still be achieved.

Information theoretic security has two striking benefits over conventional cryptography

1. no computational assumptions: useful to
   - governments worried about require long-term security.
   - organizations worried about quantum computing.
2. no keys and hence no key distribution: useful when
   - vulnerable, low-power devices are proliferating.
   - key distribution and key management obstruct security.

Practical challenge

We need definitions that yield information theoretic security in applications.

- Government-sponsored Ziva Corporation [Cor] is using optical techniques to build a receiver channel so that wiretapping results in a degraded channel.

Moving forward

- Develop practical codes that achieve the secrecy capacity under these definitions.
- Design new models for different security problems that exploit uncertainity by physical means.

References I

Ziva Corporation, *http://www.ziva-corp.com/*.

Ueli M Maurer, *Secret key agreement by public discussion from common information*.

Claude E Shannon, *The mathematical theory of communication*.

Aaron D Wyner, *The wire-tap channel*.