Information Theoretical Security

N.Cai

University of Bielefeld

26 Sep.,2011

1. Two Approaches to Security

2. Measurements and Criterions of ITS

3. Examples

Two Approaches to Security

Computational Security (CS) vs Information Theoretical Security (ITS)

Assumptions

- CS: wiretapper has limited computational ability
- ITS: wiretapper has unlimited computational ability

Security

- CS: relatively secure;
- ITS: absolutely secure

Resources (Random key, throughput, complexity, etc)

- CS: less;
- ITS: more

Two Approaches to Security

Consequence

- CS:very popular, especially in commercial systems;
- ITS: not so popular

But ITS received more and more attention. In particular CS would be broken if the wiretapper could use quantum computer.

Shannon Information Quantities

- Shannon Entropy:a measurement of uncertainty of random variable (r.v.)
  Let S be a r.v.taking values in $\mathcal{S}$. Then
  $$H(S) = -\sum_{s \in \mathcal{S}} P(S = s) \log(S = s)$$
  $$0 \leq H(S) \leq \log |\mathcal{S}|.$$
  Uncertainty may not be negative.
- Conditional Entropy: the remaining uncertainty of r.v.S if r.v. Y is known
  $$0 \leq H(S|Y) = H(S,Y) - H(Y) \leq H(S),$$
  $H(S|Y) = H(S)$ iff S and Y are independent and
  $H(S|Y) = 0$ iff S is a function of Y.
  Knowledge of Y reduces the uncertainty of S
  Note: quantum conditional entropy may be negative.

Shannon Information Quantities

- Mutual Information: Information of S contained by Y.

$$I(S;Y) = H(S) - H(S|Y) = H(S) + H(Y) - H(S,Y) = I(Y;S)$$

$$0 \leq I(S;Y) \leq H(S)$$

  $I(S;Y) = 0$ iff $H(S|Y) = H(S)$ i.e.,S and Y are independent, and $I(S;Y) = H(S)$ iff S is a function of Y.
- Similarly we have conditional mutual information $I(S;Y|X)$.

Usually we use Shannon Information Quantities to measure classical ITS but sometimes other information quantities (e.g., Rényi entropy) also are used. For quantum systems von Neumann Entropy and Holevo quantity are good measurements of security.

Criterions of ITS

- Perfect Security: the wiretapper has NO information about the secret message S, from the accessed massage Y by him, which usually take "too much" resource:

$$H(S|Y) = H(S) \text{ or } I(S;Y) = 0.$$

- Imperfect Security: the wiretapper may has LIMITED information about S, which may need less resource.

$$H(S|Y) \geq h \text{ or } I(S;Y) \leq i$$

for some $h \in (0, H(S)], i \in [0, H(S))$.

- Asymptotically Perfect (Imperfect) Security, which sometimes is easier to be handled

$$\lim_{n \to \infty} \frac{1}{n} I(S_n; Y_n) = 0.$$

The Goal to Study ITS

Look for optimal coding schemes with given secure criterion in the sense

- to maximize the protected message or throughput
- to minimize the resource needed (size of random key, etc).

Shannon Cipher System

- A random message S and a random key K are independently and uniformly generated from the same set $\{0, 1, \ldots, p-1\}$;
- The sender sends the outcomes of the random key k to the legal receiver via a secure channel;
- $m + k \ (mod\ p)$ is sent publically and both legal and illegal receivers can observe it;
- With the key the legal user may recover the message whereas without the key the illegal user has no information about S (*perfect security*).
- The size of key is equal to the size of the message.

Shannon Cipher System

The coding scheme is optimal in the sense to minimize the key size.
Proof: Shannon, 1949
The legal receiver can decode correctly $\Rightarrow H(S|Y,K)=0$
The illegal receiver has no information about $S \Rightarrow$
$H(S|Y)=H(S)$

$$\begin{aligned}\log|\mathcal{S}| &= H(S)=H(S|Y)-H(S|Y,K)\\ &= I(S;K|Y)\le H(K|Y)\le H(K)=\log|\mathcal{K}|,\end{aligned}$$

where Y is the public message.

Secret Sharing

Secret Sharing (Blakley 1979, Shamir 1979)

- There are a dealer and a set of participates in the game.
- The dealer observes a secret message S and accordingly chooses random sharings Y_i's and distributes them to participates.
- A subset of participates try to recover the message by pooling their sharings.
- They can recover it if the subset is legal (i.e. in access structure).
- Otherwise they should have absolutely no information about it from their sharings (*perfect security*).
- Fixed the sizes of the sharings received by the participates, we want to maximize the size of shared message.

Secret Sharing

(k, n) *threshold secret sharing scheme* (Blakley 1979, Shamir 1979) There are totally n participates and each $r \geq k$-subset of them are legal. That is, a set of participates can recover S iff the number of participates is no less than k. *The Scheme:*

- Choose n different non-zero elements $\alpha_i, i = 1, 2, \ldots, n$ from a field $\mathcal{F}$ with at least $n+1$ elements.
- The message S is randomly generated from the same field $\mathcal{F}$
- After receiving an outcome s of S, the dealer randomly independently chooses $k-1$ elements $a_1, a_2, \ldots a_{k-1}$ and constructs a polynomial $g(x) = s + a_1 x + a_2 x^2 + \ldots + a_{k-1} x^{k-1}$.
- The dealer sends $g(\alpha_i)$ to the ith participate as the share.
- The size of message is equal to the sizes of the sharings distributed to the participates.

It is easy to show the scheme is perfect secure i.e., any $k-1$ participates have no information about S.

Secret Sharing

Theorem: The size of the message S may not be larger than the size of sharing of Y_j for any participate j if there is no useless participate. I.e., for all participate j, there is an illegal subset set J such that $J \cup \{j\}$ is legal. Consequently threshold secret sharing scheme is optimal.

Proof: J is illegal $\Rightarrow H(S|Y_i, i \in J) = H(S)$
$J \cup \{j\}$ is legal $\Rightarrow H(S|Y_j, Y_i, i \in J) = 0$, so

$$\begin{aligned}\log|\mathcal{S}| = H(S) = H(S|Y_i, i \in J) - H(S|Y_j, i \in J) \\ = I(S; Y_j|Y_i, i \in J) \leq H(Y_j|Y_i, i \in J) \leq H(Y_j) \leq \log|\mathcal{Y}_j|.\end{aligned}$$

In general case to determine the optimal secret sharing scheme is very difficult.

Wiretap Channel I

(Classical) Wiretap channel (Wyner 1975, Csiszár-Körner 1978)

- A sender sends a uniformly distributed message S via a memoryless noisy channel with two output terminals.
- A legal receiver and a wiretapper access the two outputs of the channel resp.
- The legal receiver may correctly decode with a high probability.

Wiretap Channel I

- the wiretapper has no or limited information about the message S i.e.,

  $$\lim_{n \to} \frac{1}{n} I(S; Z^n) = 0 \text{ or } \lim_{n \to \infty} \frac{1}{n} H(S|Z^n) = \frac{1}{n} \log |\mathcal{S}|$$

  (*asymptotically perfect security*)
  or limited information about the message

  $$\lim_{n \to \infty} \frac{1}{n} H(S|Z^n) \geq h,$$

  where Z^n is random output received by the wiretapper, for a constant (“equivocation“) h, (*asymptotically imperfect security*).

Wiretap Channel I

- The goal: maximizing the transmission rate
- The maximum possible rate is call the capacity. That is, C is the capacity of a wiretap channel (for asymptotically perfect security) if for all $\epsilon, \delta, \lambda > 0$ and sufficiently large n there is a block code of length n with rate $\frac{1}{n} \log |\mathcal{S}| > C - \epsilon$ such that the legal receiver can decode correctly with probability at least $1 - \lambda$ and for the wiretapper

  $$\frac{1}{n} I(S; Z^n) < \delta.$$

  and there is no such code exists if the rate $\frac{1}{n} \log |\mathcal{S}| > C$.
- Similarly one may define capacity of wiretap channel for asymptotically imperfect security. Obviously the capacity decreases if the equivocation increases.

Wiretap Channel I

The proof of the *Coding Theorem*, (or determining the capacity), is divided as two parts:

- *Direct Part:* The existence proof: By random coding. For wiretap channel, the randomization of input is necessary.
- *Converse Part:* The non-existence proof: By information inequalities.
- The additional resources. e.g., feedback, common randomness shared by the legal users etc, may increase the capacity (Ahlswede-C. 2006).
- Alternative models e.g., compound wiretap channel (Bjelaković-Boche-Sommerfeld, 2011), wiretap channel with side information (Chen-Vinck, 2008), etc, were studied.

Quantum Wiretap Channel

Classical-Quantum Wiretap Channel, (C.-Winter-Yeung 2004, Devetak 2005)

- A memoryless channel with a classical input and two quantum outputs connect a sender Alice and a legal receiver Bob and a wiretapper. That is, Bob and the wiretapper receive quantum states $\rho^{\otimes n}(x^n)$ and $\sigma^{\otimes n}(x^n)$ resp. if Alice inputs a classical sequence x^n.
- Alice sends a classical message via the channel. We want that Bob correctly decodes the message with an arbitrarily high probability and the wiretapper has no information, no mater what measurement he use. Namely the Holevo quantity between Alice and the wiretapper vanishes as length of the code increases (*asymptotically perfect security*).

Quantum Wiretap Channel

- Due to no-cloning theorem we have to describe the two quantum outputs by a single “big” state $\omega(x)$. I.e., $\rho(x) = tr_W(\omega(x))$ and $\sigma(x) = tr_B(\omega(x))$.
- It turns out that the capacity is equal to the difference of the two Holevo quantities i.e., the coherent information.
- The result had been used to prove (direct) coding theorem for quantum-quantum channel (Devetak 2005).

Wiretap Channel II

The wiretap channel II (Ozarow-Wyner 1984)

- Message is encoded into a codeword of length n via a noiseless channel.
- A legal user receives the whole codeword.
- A wiretapper accesses any t components of the codeword.
- The legal user can decode correctly (with probability one). The illegal user has no information about the message (*perfect security*), or limited information about it (*perfect security*).
- To maximize the size of the message: The problem has been completely solved. (the Direct part: by construction of code: the Converse: by information inequalities).

Wiretap Network

Wiretap Network (C.-Yeung, 2002, 2011) consists of

- a graph (nodes - users, edges - noiseless channels).
- a subset of nodes - source nodes accessing information sources and a subset of nodes - sinks accessed by legal receivers.
- a collection of subsets of channels - collection of wiretap subsets

Senders send messages from source nodes to sinks via the network and a wiretapper can arbitrarily choose wiretap subset and accesses its all channel. The requirement of coding is that the legal receiver correctly decode and the wiretapper has no or limited information about the message (*perfect and imperfect security*). The goal is to maximum the throughput and minimize the randomness used by coding.

The model contains Shannon cipher system, secret sharing, and wiretap channel II as special cases.

Private Computations in Networks

- There are n users $1, 2, \ldots, n$ in a communication network, each accesses an information source X_i. The sources are independent.
- The users cooperate to compute the value of a function $f(X_1, X_2, \ldots, X_n) := f(X^n)$ by exchanging information over the network.
- The users do not trust each others and they want the others to know no additional information about their own source. That is, the remaining uncertainty of the sources for the user j must be $H(X_i, i \neq j | X_j, f(X^n))$ after the communication (*perfect security*).
- The goal is to minimize the randomness needed.

Key Agreement

Key agreement or Key Distribution (Maurer, Ahlswede-Csiszar, Csiszar-Narayan, et al)

- A set of legal users try to generate a common secret random key by discussion through a public channel or network. The legal users and a wiretapper may observe all message sent via public channel. Usually we assume that the users may send unlimited message through the public channel.
- The wiretapper try to have as much as possible information about the key. The requirement is the wiretapper may have no information or limited information about the secret key. That is, the mutual information between the key and the message leaked to the wiretapper asymptotically vanishes or upper bounded by a given constant. (*asymptotically perfect or imperfect security*).

Key Agreement

- The legal users share certain resource whereas the he wiretapper may or may not have certain own related resource.
- By resource for legal users, we mean different terminals of a correlated information source, inputs and outputs of private channels, different parts of entanglement states, etc. The resource of wiretapper are a different terminal of of the same information source, different outputs of the same private channels and parts of the same entanglement states, etc.
- the goal is to maximize the rate of the common key.

Key Agreement

An Example of Key Agreement (Maurer 1993, Ahlswede-Csiszar 1993)

- There is a discrete memoryless correlated information source (X^n, Y^n, Z^n) in the model.
- Alice, Bob, and a wiretapper access the terminals X^n, Y^n, and Z^n of the source resp.
- Alice and Bob (the legal users) try to generate a common secrete key with a as large as possible rate by discussion via a public channel according to the outcomes of X^n and Y^n such that the wiretapper has no or limited information about the key (*asymptotically perfect or imperfect security*).
- The otimal coding shceme was obtained.

Key Agreement

A Quantum Application of the Coding Scheme in the Example (Schumacher-Westmoreland, 1998)

- Alice assesses the classical input of a memoryless classical-quantum wiretap channel and Bob and a wiretapper access the two quantum outputs of the channel resp. Alice and Bob generate a common random key by the following scheme.
- Alice random chooses a classical input X^n according to a *i. i. d.* distribution P^n and sends it through the channel.

Key Agreement

- Bob and the wiretapper perform measurement to their own outputs, *components by components* repeatedly, and to have random sequences Y^n and Z^n resp. This builds *meoryless* correlated source (X^n, Y^n, Z^n) accessed by Alice, Bob, and the wiretapper.
- Then Alice and Bob apply the coding scheme in the example to generate a random key with rate $I(X;Y) - I(X;Z)$ such that *Shannon mutual information* between the key and all messages received by the wiretapper vanishes as the length of the code increases (*asymptotically perfect security*).

Key Agreement

An Observation on the Application (C.-Winter-Yeung, 2004): The strategies for both sides are not optimal.

- It actually formes a classical wiretap channel (I) if Bob and the wiretapper apply the strategy to measure their quantum outputs components by components. Thus Alice may first randomly generate a key and then treat the (resulting) channel as a classical channel to send the key via it, with a rate at least $I(X;Y) - I(X;Z)$ (sometimes even larger). That is, the public discussion is Not necessary in this case.
- The strategy to measure the quantum output component by component for the wiretapper is not optimal. In fact it has been shown that the wiretapper may have a better result by performance of a suitable measurement to the *whole output* (see the next slide).

Key Agreement

- More severely to apply the coding scheme for key agreement with 3 terminal source, Alice and Bob must know the joint distribution of the correlated source. In other words, Alice and Bob must know the both measurements, of Bob and the wiretapper, before choosing a code. For no reason the wiretapper to inform them his own measurement.
- For the same reason,we must know wiretapper's measurement if we stick to use a particular Shannon conditional entropy to measure the security. On the other hand the wiretapper may perform a good measurement to the *whole output* asymptotically to achieve the Holevo bound, the upper of information for all measurement, which may not be achieved by Shannon mutual information obtained by measurement component by component.Thus in this case, Holevo quantity is a better measurement of security.

Key Agreement

- Similarly Bob also may perform a measurement to whole his output instead of the measurements component by component.
- This motivated us to study classical-quantum wiretap channel. By employing a secure code for the channel Alice and Bob may achieve the coherent information, the best possible key rate in both cases with and without public discussion. It is secure no mater what measurement the wiretapper chooses. That is the public discussion is unnecessary.

Thank You!