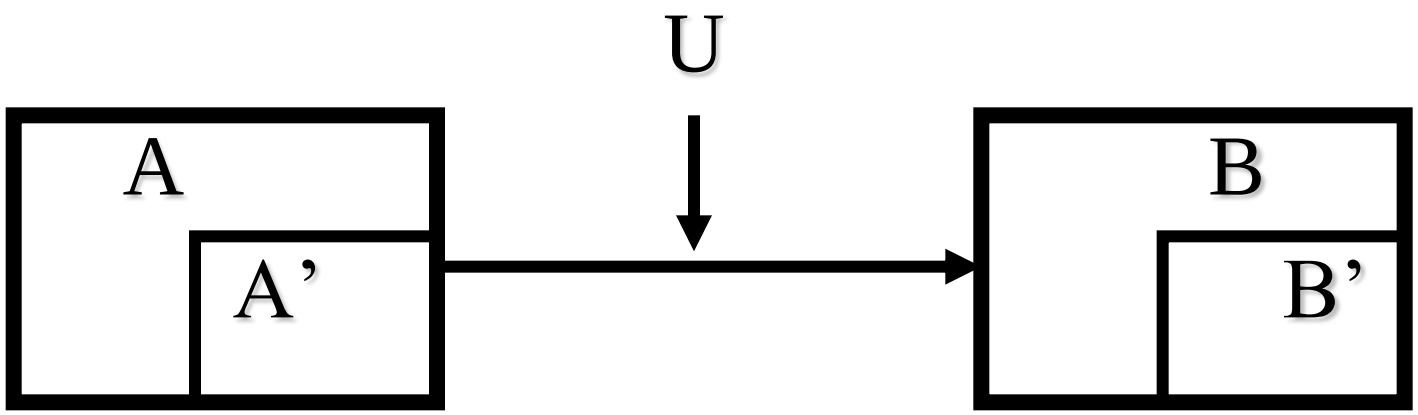
Problems of Modeling in the Analysis of Covert Channels

A. Grusho, N. Grusho, E. Timonina

September 8-11, 2010, St. Petersburg, Russia

International Conference "Mathematical Methods, Models and Architectures for Computer Network Security"

Problems of Modeling in the Analysis of Covert Channels



Transition of hidden information from A’ to B’ should be consistent with legal information transmission. The main task of U is to discover existence of hidden information.

Problems of Modeling in the Analysis of Covert Channels

U decides that there is hidden information when the transmitted sequence belongs to a predefined set ***S***.

If U does not know how to define ***S***, then hidden transmission from A' to B' is "invisible" for U.

Problems of Modeling in the Analysis of Covert Channels

A' invents his method of hiding information in such a way that U has no reason to choose ***S***.

Example. Let legal information is chosen with probability measure P_0 . A' knows P_0. If A' can hide information in such a way that the transmitted information has probability distribution P_0, then U has no base to choose ***S***.

Problems of Modeling in the Analysis of Covert Channels

If A' thinks that the legal information distribution is P_0 , but the real probability distribution is Q_0, then U can get a chance to catch hidden transmission.

Define **ban** be a minimal finite subsequence that the presence of this subsequence in any finite sequence means that the probability P_0 of this sequence equals to 0.

Problems of Modeling in the Analysis of Covert Channels

If A’ doesn’t know about existence of a ban but U knows it, then U builds a simple decision function: he waits for appearance of the ban.

A ban maybe introduced into probability distribution intentionally.

There can be many bans in legal distribution.

Problems of Modeling in the Analysis of Covert Channels

Then:

1. We can defend legal transmission with help of bans.
2. If A' doesn't know the choice of a ban and he intends to send a sequence which doesn't belong to ***S***, then it can happen that he has no choice.

Problems of Modeling in the Analysis of Covert Channels

Mathematical properties of bans

1. If P_0 doesn't have a ban and we introduce it into P_0 , then topological structure of the measure support changes deeply.
2. It can be proved that if consistent sequence of tests for separation of legal and hidden transmission exists, then the decision may be built on a search of bans.
3. Most often the set of bans may be constructed by analyzing of probability distribution of a limited part of random sequences.