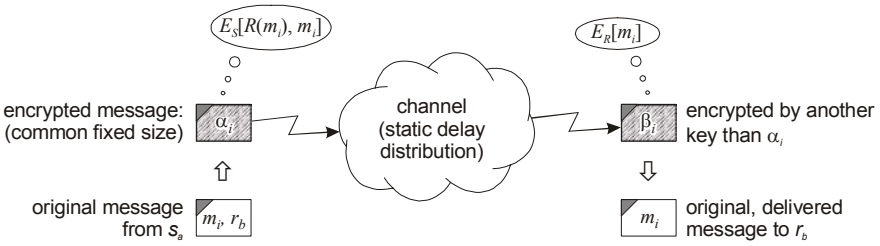
Measuring Anonymity in a Passive, Real-time System

Gergely Tóth, Zoltán Hornák
Budapest University of Technology and Economics
Department of Measurement and Information Systems
{tgm,hornak}@mit.bme.hu

Anonymous message transmission should be a key feature in network architectures. It should ensure that delivered messages are impossible — or at least infeasible — to be traced back to their senders. For this purpose several techniques exist (such as MIX-nets or Onion Routing). For theoretical analysis the model of the PROB-channel was defined. It is designed concerning three main aspects: it should offer guaranteed message transmission throughput; an objective, theoretical measure should be offered for the achieved anonymity; and requirements should be defined for reaching a given level of anonymity.

With the above requisites in mind the PROB-channel is defined as follows: the transmission channel is a passive system (its behavior is not affected by the message distribution), it is real-time (message delay has a guaranteed maximum), is observable (the adversary may eavesdrop on all communication channels) and is black-box (thus no internal information leaks out of the system). Messages from the senders enter the channel in an encrypted form α_i and they will be delivered to the recipients as β_i-s encrypted with different keys (see figure below). Message delay in the channel is a probability variable δ with a given distribution while it is time and message invariant.



As an adversary a passive observer was analyzed. This observer is able to eavesdrop on all communication channels of the system, knows the potential senders and recipients and all the public parameters of the channel. In order to break the anonymity of the system the observer calculates the probability of a certain delivered message being sent by a certain sender. Based on this observer's characteristics two methods have been considered: the observer might perform a global back-tracing by selecting the most probable match from all possible match combinations of delivered and sent messages (this approach may be unfeasible in practice since it is exponential) or he can apply local back-tracing and calculate the possible senders of each delivered message independently. For our conclusions the second approach was chosen since only this one is feasible for practical scenarios.

Based on the above considerations two theoretical measures can be defined for the system: for the sender-anonymity the source-hiding property with parameter Θ (if the observer cannot link any delivered message to a sender with a probability greater than Θ) and for the recipient-anonymity the destination-hiding property with parameter Ω (if the observer cannot link any recipient for a sent message with a probability greater than Ω).

Finally in order to achieve guaranteed level of sender-anonymity the MIN/MAX property was introduced in our model: by enforcing senders to obey rules (specifying a frequency range for message sending intensity) upper limit can be given for the Θ of the destination-hiding property. However for achieving the optimum in the model another aspect has to be considered: the distribution of the delay probability variable has to be uniform. By combining these two methods the anonymity level of the system becomes independent of the actual message distribution and thus a guaranteed level of anonymity can be provided.