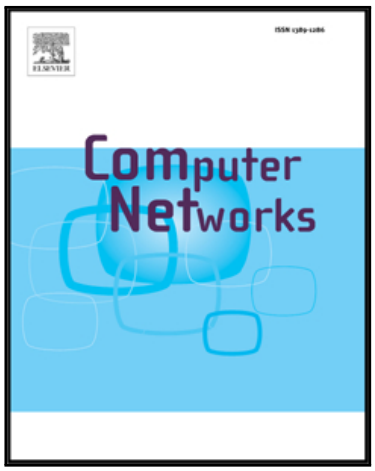

Reliable and Perfectly Secret Communication over the Generalized Ozarow-Wyner's Wire-Tap Channel

Giulio Aliberti, Roberto Di Pietro, Stefano Guarino

PII: S1389-1286(16)30214-6
DOI: 10.1016/j.comnet.2016.06.034
Reference: COMPNW 5952

To appear in: *Computer Networks*

Received date: 14 October 2015
Revised date: 9 May 2016
Accepted date: 26 June 2016

Please cite this article as: Giulio Aliberti, Roberto Di Pietro, Stefano Guarino, Reliable and Perfectly Secret Communication over the Generalized Ozarow-Wyner's Wire-Tap Channel, *Computer Networks* (2016), doi: 10.1016/j.comnet.2016.06.034

Reliable and Perfectly Secret Communication over the Generalized Ozarow-Wyner's Wire-Tap Channel

Giulio Aliberti[a,b], Roberto Di Pietro[a,d,*], Stefano Guarino[c]

[a] *Security Research, Nokia Bell Labs, Paris-France*
[b] *Università di Roma Tre, Dip.to di Matematica, Roma-Italy*
[c] *Istituto per le Applicazioni del Calcolo "Mauro Picone" (IAC), Consiglio Nazionale delle Ricerche (CNR)*
[d] *Università di Padova, Dip.to di Matematica, Padova-Italy*

Abstract

In a typical secure communication system, messages undergo two different encodings: an error-correcting code is applied at the physical layer to ensure correct reception by the addressee (integrity), while at an upper protocol layer cryptography is leveraged to enforce secrecy with respect to eavesdroppers (confidentiality). All constructive solutions proposed so far to concurrently achieve both integrity and confidentiality at the physical layer, aim at meeting the secrecy capacity of the channel, *i.e.*, at maximizing the rate of the code while guaranteeing an asymptotically small information leakage.
In this paper, we propose a viable encoding scheme that, to the best of our knowledge, is the first one to guarantee both perfect secrecy (*i.e.*, no information leakage) and reliable communication over the *generalized* Ozarow-Wyner's wire-tap channel. To this end, we first introduce a metric called *uncertainty rate* that, similarly to the *equivocation rate* metric, captures the amount of information leaked by a coding scheme in the considered threat model, but it is simpler to apply in the context of linear codes. Based on this metric, we provide an alternative and simpler proof of the known result that no linear error-correcting code alone can achieve perfect secrecy. Finally, we propose a *constructive* solution combining secret sharing and linear error-correcting codes, and we show that our solution provides the desired combination of reliable and perfectly secret communication. The provided solution, other than being supported by thorough analysis, is viable in practical communication systems.

Keywords: Physical Layer Security, Wire-Tap Channel, Perfect Secrecy, Error-Correcting Codes, Secret Sharing

*Corresponding author. Tel.: +33 (0)1 6040 8110; fax: +33 (0)1 6040 8001
Email addresses: aliberti@mat.uniroma3.it (Giulio Aliberti), roberto.di_pietro@nokia.com (Roberto Di Pietro), s.guarino@iac.cnr.it (Stefano Guarino)