SaTC: CORE: Small: A Practical Approach to Study Security in Wireless Networks

Hamid Bahrami, Nghi Tran, Mehdi Maleki, The University of Akron

https://www.nsf.gov/awardsearch/showAward?AWD_ID=1956110

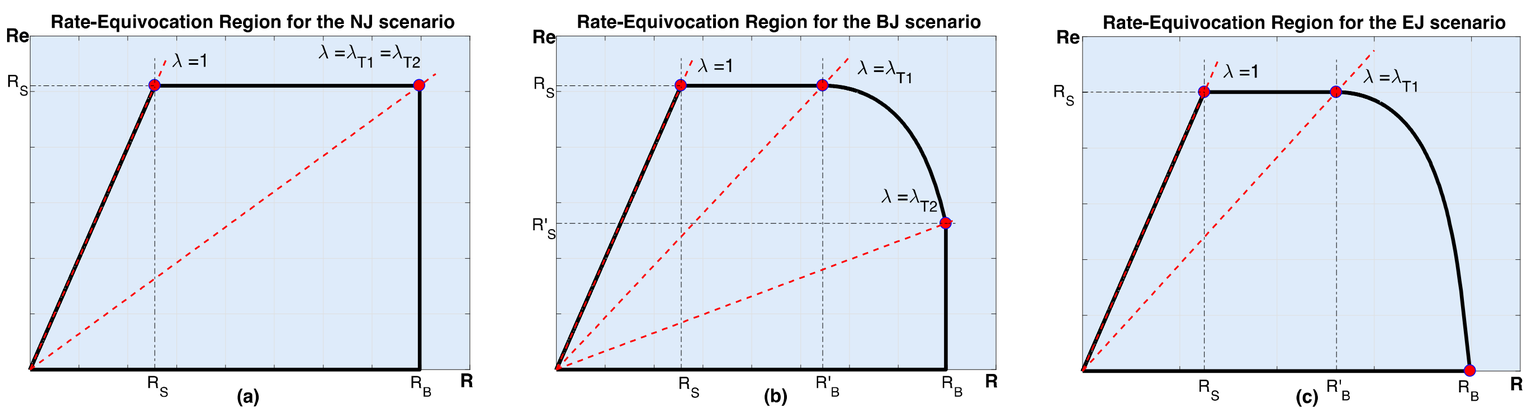
We propose a novel framework to study the joint effect of physical layer security (PhySec) and encryption. Such a framework relies on the concept of rate-equivocation regions and can be used to study the tradeoff between encryption strength, allowed leakage, and transmission rate. By considering encryption, it is possible to achieve transmission rates beyond the secrecy capacity that is achievable by conventional physical layer security. Toward our goal, we exploit the fact that cryptography undermines the ability of the eavesdropper to access the plaintext. We then relax the design of physical layer security schemes without compromising the security of the system.

Despite several recent advances in PhySec, there is still no clear path to connect the PhySec to cryptographic security (CryptoSec). In fact, conventional PhySec designs in the literature generally neglect the existence of CryptoSec at higher layers of the protocol stack. In conventional PhySec, the designs are based on the assumption of unlimited computational power at the eavesdropper, which means that the presence of the encryption is completely ignored. On the other hand, unlike classical encryption, it is assumed that the eavesdropper cannot at all retrieve the correct cipher message. In other words, in PhySec, the eavesdropper is assumed weak in interception but strong in computation. To invent more powerful PhySec schemes that use the system resources more efficiently, it is imperative to take into account the impact of encryption in their design. By establishing a connection between PhySec and CryptoSec, it will be possible to come up with highly promising PhySec solutions to achieve a more flexible trade-off of critical system resources.

Our framework establishes a connection between transmission rate, equivocation rate, and encryption strength. We show that to have a secure transmission, we should have $\frac{R_e}{R} \geq \frac{1}{\lambda}$.
In this equation, R and Re are the transmission and equivocation rates, respectively, and λ is a parameter that measures the encryption strength. λ is inversely proportional to the minimum error probability required for an eavesdropper to fail in breaking the cipher. The encryption-aware secrecy rate for a wiretap channel (WTC) can then be derived as the solution to the following optimization problem:

$$\bar{R}_S \triangleq \sup_R \left\{ R : \left(R, \frac{R}{\lambda} \right) \in \bar{\mathcal{R}}^{WTC} \right\}.$$

Typical rate-equivocation regions for a 4-node WTC (transmitter, receiver, jammer, and eavesdropper); the red lines show the threshold for encryption strength



Secure transmission rate for 3- and 4-node WTCs with and without encryption awareness